Manuale Operativo del Servizio TIM ID in ambito SPID

(Sistema Pubblico di gestione delle Identità Digitali ai sensi del DPCM 24 ottobre 2014)

MANUALE OPERATIVO

Indice degli argomenti

1 Informazioni generali

1.1 Dati identificativi della versione del manuale

Versione	Data	Descrizione delle modifiche rispetto alla precedente emissione
00	15/09/2015	Prima emissione
01	29/02/2016	Aggiunto canale 'Help Desk Telefonico' tra le modalità di interazione con l'Utente (paragrafo 4.2). Aggiunte le modalità di Identificazione mediante Firma Elettronica Qualificata o Digitale (paragrafo 5.2.2.2) e mediante Carta CNS o CIE (paragrafo 5.2.2.3), per le Persone Giuridiche. Integrato capitolo 8 e paragrafo 8.1 per introduzione modalità di Identificazione mediante Firma Elettronica Qualificata o Digitale e modalità di Identificazione mediante Carta CNS o CIE, per le Persone Giuridiche. Aggiunta la modalità di 'Sospensione Telefonica' nella Gestione del ciclo di vita dell'Identità Digitale (paragrafo 9.5.1.2).
02	10/10/2016	Integrati i paragrafi 1.4 e 4.2 per l'avvio della distribuzione del servizio nell'ambito dell'offerta del Gruppo TIM. Integrati il paragrafo 2.5, il paragrafo 5.1 e sottoparagrafi 5.1.1.2, 5.1.2.2 per introduzione modalità di Identificazione mediante Sistemi di Registrazione Audio-Video, per le Persone Fisiche e le Persone Giuridiche. Aggiunta la modalità di Identificazione mediante Sistemi di Registrazione Audio-Video per le Persone Fisiche (paragrafo 5.2.1.4) e per le Persone Giuridiche (paragrafo 5.2.2.4). Integrato il capitolo 8 e paragrafo 8.1 per introduzione modalità di Identificazione mediante Sistemi di Registrazione Audio-Video, per le Persone Fisiche e le Persone Giuridiche. Integrato il par. 12.1 a seguito dell'emissione di nuove disposizioni normative.
03	26/05/2017	Integrato paragrafo 2.5 con descrizione controlli anticontraffazione eseguiti sulla documentazione di Identificazione. Integrato paragrafo 9.4.1 per introduzione motivazione di revoca da parte del Gestore per scadenza documentazione di identificazione.
04	27/07/2017	Integrati paragrafi 5.1.1.2 e 5.1.2.2 per introduzione nel processo di Registrazione della funzionalità di upload della versione digitalizzata della documentazione di identificazione, per la modalità 'de-visu'. Integrati paragrafi 5.2.1.1 e 5.2.2.1 per introduzione nella modalità di identificazione 'de-visu' del provisioning certificato di FEA associato a Richiedente identità digitale. Integrato paragrafo 9.1 per introduzione funzionalità di visualizzazione e download dei documenti personali e contrattuali del titolare (nuovo sottoparagrafo 9.1.1).
05	25/05/2018	Aggiornati i riferimenti normativi in occasione dell'entrata in vigore del Regolamento Generale sulla Protezione dei Dati n. 2016/679/UE. Aggiornato paragrafo sul prezzo del servizio. Aggiornato con riferimenti a TIM Digital Store al posto di TIM Nuvola Store. Inserito registrazione a TIM Digital Store come prerequisito per la linea di attivazione basata su TIM Digital Store. Inserito l'impegno a informare l'utente dei cambiamenti nelle condizioni d'utilizzo o nell'informativa privacy. Aggiornato per nuova piattaforma CA.

06	02/10/2019	Aggiornato il rappresentante legale (par. 1.3). Eliminato riferimento alla necessità di registrazione preventiva al sito Digital Store TIM (par. 4.2). Specificazione che non le firme digitali basate su certificati con OID 1.3.76.16.5 (firma ottenuta tramite SPID) non possono essere usate per identificarsi a SPID (par. 5.2.1.2). La ID sospesa su richiesta utente se non revocata rimane sospesa fino a scadenza naturale (parr. 4.1.1, 9.4.1, 9.5.1.3 e 9.6.1.1). Eliminati tutti i riferimenti al livello di autenticazione L3 SPID in quanto non disponibile nel servizio. Aggiornamento dei riferimenti della normativa Privacy al GDPR (par. 12.1).
07	04/06/2021	Aggiunta linea di attivazione de-visu presso i negozi TIM (par. 5.2.1.2) Editing del documento
08	11/09/2024	Allineamento e aggiornamento della documentazione del servizio

1.2 Scopo del documento

Questo documento illustra le regole generali e le procedure seguite dal Gestore di Identità Digitale **Telecom Italia Trust Technologies S.r.l.** (in breve TI Trust Technologies o TITT o Identity Provider o Gestore) nell'erogazione del servizio TIM ID (in breve anche SERVIZIO) nell'ambito del Sistema Pubblico per l'Identità Digitale italiano (SPID) in conformità alla normativa italiana (v. cap. 13 per i tutti i rifermenti).

Il presente documento:

- è pubblicato a garanzia dell'affidabilità del SERVIZIO nei confronti dei soggetti operanti nell'ambito dello SPID;
- contiene la descrizione delle modalità operative del SERVIZIO;
- costituisce documento pubblico secondo la disciplina emanata da AgID;
- è liberamente disponibile per la consultazione ed il download in apposita sezione del sito del Gestore: http://www.trusttechnologies.it nonché sul sito AgID (http://www.agid.gov.it).

1.3 Identificazione del Gestore e del Responsabile del Manuale Operativo

La società TI Trust Technologies s.r.l., con unico socio, Gruppo Telecom Italia, è già accreditata presso AgID in qualità di Gestore di Posta Elettronica Certificata, di Certificatore Accreditato della Firma Digitale e della CNS e di Conservatore Accreditato.

TI Trust Technologies risponde alla Direzione del Gruppo Telecom Italia per il tramite della Società Olivetti che ne ha la proprietà, nel cui ambito ha la responsabilità di assicurare la commercializzazione e lo sviluppo di servizi a valore aggiunto in materia di sicurezza informatica, fra i quali rientrano in modo specifico tutti i servizi che essa eroga.

Di seguito i dati identificati di TI Trust Technologies:

Denominazione e Ragione Sociale	**Telecom Italia Trust Technologies S.r.l.**
Rappresentate legale (Amministratore Delegato)	Luciano Albanese
Sede Legale	S.R.148 Pontina, km. 29,100 00071 - Pomezia (RM)
Sede Operativa	S.R.148 Pontina, km. 29,100

	00071 - Pomezia (RM)
Indirizzo PEC	ti.tt@ttpec.telecomitalia.it
Indirizzo di Posta elettronica	info-ttstore@telecomitalia.it
Indirizzo Internet	http://www.trusttechnologies.it

Il responsabile del Manuale Operativo è **Simone Storico.**

1.4 Destinatari e tariffe del Servizio

La distribuzione sul mercato del SERVIZIO è effettuata da TI Trust Technologies o dalle Società Telecom Italia S.p.A. (in breve TIM), in virtù di specifici accordi contrattuali.

I destinatari dell'offerta commerciale sono gli utenti dello SPID, ovvero le persone fisiche e giuridiche interessate ad operare nello SPID.

Il SERVIZIO è fornito alle seguenti condizioni economiche:

- l'identità digitale associata ai livelli SPID 1 e 2 **si intende rilasciata a titolo gratuito** agli utenti persone fisiche (Tipo 1 SPID) che utilizzano le modalità di identificazione de visu, firma digitale o CNS. Per le altre modalità messe a disposizione dell'utenza, il Gestore potrà prevedere dei corrispettivi per l'effettuazione delle attività di identificazione, come indicati nella documentazione informativa che sarà resa disponibile sul sito del Gestore o di TIM.
- l'identità digitale associata ai livelli SPID 1 e 2 si intende rilasciata a titolo oneroso a tutti gli utenti persone giuridiche (Tipo 2 SPID);

1.5 Ambito di applicazione

Il SERVIZIO erogato dal Gestore e l'ambito di applicazione del presente manuale operativo fanno riferimento esclusivamente al rilascio e alla gestione delle Identità Digitali SPID (Sistema Pubblico dell'Identità Digitale), in qualità di Identity Provider (IdP).

2 Obblighi del Gestore dell'Identità Digitale SPID e del Titolare dell'Identità Digitale SPID

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

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

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

2.1.1 Obblighi del Gestore

Descrizione
Rilasciare l'identità su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta, nelle modalità più oltre indicate.
Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale.

Conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione *de visu.*
Conservare copia del log della transazione nei casi di identificazione tramite documenti digitali di identità, identificazione informatica tramite altra identità digitale SPID o altra identificazione informatica autorizzata.
Conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso si identificazione tramite firma digitale.
Verifica degli attributi identificativi del richiedente.
Consegnare in modalità sicura le credenziali di accesso all'utente.
Conservare la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale.
Cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale.
Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui alla [Normativa Privacy].
Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione.
Effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso.
Revocare l'identità digitale se ne riscontra l'inattività per un periodo superiore a 24 mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica.
Segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente.
Verificare la provenienza della richiesta di sospensione da parte dell'utente (escluso se inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata).
Fornire all'utente che l'ha inviata conferma della ricezione della richiesta di sospensione.
Sospendere tempestivamente l'identità digitale ed informarne il richiedente.
Rispristinare o revocare l'identità digitale sospesa, nei casi previsti.
Revocare l'identità digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione.
Utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale.
Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso.
Effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta.
Effettuare con cadenza almeno annuale un'analisi dei rischi.
Definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID.
Allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato.
Condurre con cadenza almeno semestrale il *Penetration Test.*
Garantire la continuità operativa dei servizi afferenti allo SPID.
Effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna.

Garantire la gestione sicura delle componenti riservate delle identità digitali assicurando non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata.
Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa.
Sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti.
Informare tempestivamente l'AGID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali.
Adeguare i propri sistemi a seguito dell'aggiornamento della normativa.
Inviare all'AGID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici.
In caso intendesse cessare la propria attività, comunicarlo all'AGID almeno 30 giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le identità digitali rilasciate.
In caso di subentro ad un gestore cessato, gestire le identità digitali che questi ha rilasciato dal gestore cessato e conservarne le informazioni.
In caso di cessazione dell'attività, scaduti i 30 giorni, revocare le identità digitali rilasciate e per le quali non si è avuto subentro.
Informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi.
Se richiesto dall'utente, segnalargli via e-mail o via sms, ogni avvenuto utilizzo delle sue credenziali di accesso.
Notificare all'utente la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua identità digitale.
Nel caso l'identità digitale risulti non attiva per un periodo superiore a 24 mesi o il contratto sia scaduto, revocarla e informarne l'utente via posta elettronica e numero di telefono mobile.
In caso di decesso del titolare (persona fisica) o di estinzione della persona giuridica, revocare previo accertamento l'identità digitale.
Nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.
Trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, mantenere l'identità sospesa sino alla sua revoca per inattività qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione.
Nel caso in cui l'utente richieda la sospensione o la revoca della propria identità digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'identità digitale.
Mantenere l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente.
In caso di richiesta di revoca di dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale.
Proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa.
All'approssimarsi della scadenza dell'identità digitale, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta.

In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.
Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID.
Tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, inalterabilità e integrità, adottando idonee misure di sicurezza ed utilizzando meccanismi di cifratura in conformità alla [Normativa Privacy].

2.1.2 Obblighi del Titolare dell'Identità Digitale

Descrizione
Esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione.
Si obbliga all'uso esclusivamente personale delle credenziali connesse all'Identità Digitale.
Si obbliga a non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti. A tale proposito, si precisa che l'utente è tenuto ad adottare tutte le misure tecniche e organizzative idonee ad evitare danni a terzi.
Si obbliga a non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine.
Deve garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi.
L'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private.
Sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite.
Fornire/comunicare al Gestore dati ed informazioni fedeli, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci.
Accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze.
Informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati.
Mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi: • se persona fisica: estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale, • se persona giuridica: indirizzo sede legale, codice fiscale o P.IVA, rappresentante legale della società, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale.
Conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i rischi seguenti: • divulgazione, rivelazione e manomissione • furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'identità digitale • accertarsi dell'autenticità del fornitore di servizi o del gestore dell'identità digitale quando viene richiesto di utilizzare l'identità digitale.
Attenersi alle indicazioni fornite dal Gestore in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca delle credenziali, alle cautele che da adottare per la conservazione e protezione delle credenziali.

In caso di smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria) richiedere immediatamente al Gestore la sospensione delle credenziali.
In caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto richiedere immediatamente al Gestore la sospensione delle credenziali.

2.1.3 Responsabilità del Gestore

Il Gestore è responsabile verso l'utente per l'adempimento di tutti gli obblighi derivanti dall'espletamento delle attività richieste dalla normativa vigente in materia di Sistema Pubblico di Identità Digitale.

In particolare, nello svolgimento della sua attività:

Descrizione
Attribuisce l'Identità Digitale e rilascia le credenziali connesse attenendosi alle Regole Tecniche emanate dall'AGID.
Si attiene alle misure di sicurezza previste dal "Codice in materia di protezione dei dati personali" ai sensi della [Normativa Privacy] nonché alle indicazioni fornite nell'informativa pubblicata sul sito https://www.trusttechnologies.it/.
Procede alla sospensione o revoca delle credenziali in caso di richiesta avanzata dall'utente per perdita del possesso o compromissione della segretezza, per provvedimento dell'AGID o su propria iniziativa per acquisizione della conoscenza di cause limitative della capacità dell'utente, per sospetti di abusi o falsificazioni.
Informa i titolari di Identità Digitali in modo tempestivo e affidabile delle eventuali modifche alla definizione del servizio e ai termini, alle condizioni e all'informativa sulla privacy applicabili al servizio SPID.

3 Cenni sulle infrastrutture del Gestore

Per l'erogazione del SERVIZIO il Gestore utilizza sistemi riservati allo scopo, situati in locali adeguatamente protetti, per i quali sono riportati gli aspetti più rilevanti:

- La piattaforma è stata progettata in modo da garantire nel tempo la capacità di incrementare gradualmente nel tempo la performance e la capacità di produzione attraverso l'espansione delle infrastrutture via via necessarie
- La piattaforma di erogazione del SERVIZIO adotta soluzioni **hardware** e **software** selezionate per garantire interoperabilità, affidabilità e sicurezza;
- La continuità del SERVIZIO è garantita grazie a sistemi di **ridondanza funzionale** e di **disaster recovery**;
- TI Trust Technologies dispone di un pool di risorse avente uno specifico know-how sulle tecnologie dei servizi trusted e delle strutture di PKI, continuamente aggiornato attraverso attività di scouting e di contatto con i principali vendor del settore. Il Competence Center di TI Trust Technologies può vantare una collaborazione pluriennale con AgID e con altri enti italiani e stranieri (i.e. Assocertificatori).

L'infrastruttura per l'erogazione del SERVIZIO del Gestore è organizzata logicamente su cinque componenti:

- Il **Sistema di Autenticazione** provvede all'autenticazione dei soggetti che accedono al SERVIZIO, gestita tramite policy configurabili. Ogni componente della struttura è ridondato e configurato per garantire elevati livelli di sicurezza e riservatezza dei dati;
- La **Componente di Front-End** realizza tutte le funzionalità necessarie alla gestione degli strumenti e del ciclo di vita delle identità digitali: esposta su Internet/Intranet, è l'unica componente autorizzata a colloquiare con la componente di Back-End posta nella zona protetta (DMZ);
- La **Componente di Back-End** è inserita nella zona più protetta della rete del Gestore e non viene esposta all'esterno (ossia non è per nessuna ragione raggiungibile direttamente da Internet): fornisce le funzionalità fondamentali della piattaforma e dei servizi del Gestore;

- La **Rete di Gestione** permette agli operatori del Gestore di raggiungere i sistemi posti sulle reti di Front-End e Back-End per le attività di gestione: tale rete è posta all'interno della Sala Sistemi del Centro Servizi del Gestore e non è raggiungibile dall'esterno; gli accessi ai sistemi sono effettuati in modalità sicura tramite sessioni SSH con accesso controllato da FIREWALL e autenticazione centralizzata Active Directory/LDAP;
- **Rete di backup**: garantisce il servizio di salvataggio ed archiviazione dei dati.

Fra le principali **misure di sicurezza** che vengono adottate per garantire che le attività del Gestore si svolgano secondo i requisiti richiesti dalla normativa vigente, si ricordano:

- i meccanismi per il controllo dell'accesso logico e fisico alle risorse e ai sistemi del Gestore, che forniscono le seguenti funzionalità:
  - identificano ed autenticano le persone autorizzate ad accedere alle risorse,
  - impediscono ad una persona non autorizzata di poter accedere alle risorse,
  - registrano i dati significativi di tutti gli eventi di accesso in modo che si possa in ogni caso risalire alla persona che ha dato origine ad un determinato evento;
- il controllo dell'accesso ai locali protetti adotta una politica di autorizzazioni e di procedure di registrazione e auditing;
- l'accesso alla Sala Sistemi del Centro Servizi del Gestore è consentito al solo personale autorizzato del gestore e controllato da sofisticati sistemi di identificazione (es. rilevazione biometrica): ogni persona che intende accedere alle risorse della Sala Sistemi è identificata in modo certo, mediante l'utilizzo di strumenti di identificazione o mediante complesse procedure di identificazione (es. smartcard, token personale);
- in particolare, ogni attività di ciascuna sessione nei sistemi del gestore è registrata in appositi audit-log.

Le caratteristiche di dettaglio della gestione della sicurezza del Gestore sono contenute nel corrispondente Piano della Sicurezza e non sono oggetto di divulgazione.

3.1 Descrizione dell'architettura di erogazione del Servizio

TI Trust Technologies nella scelta della migliore soluzione utile a realizzare la propria piattaforma di Identity Provider si è basato sulla ricerca di tecnologie di mercato già predisposte per offrire servizi innovativi ed ad alto valore aggiunto.

La soluzione adottata è modulare e altamente scalabile e la piattaforma di erogazione è realizzata con un'architettura robusta ed in alta affidabilità.

Il SERVIZIO è realizzato ad hoc, implementato e configurato in conformità alle regole tecniche e agli standard richiesti dalla normativa.

La soluzione implementata è strutturata su 3 livelli principali (tier) della che separano, logicamente e/o fisicamente, le componenti del sistema. La soluzione è scalabile per garantire il *load balancing* e la *business continuity* richiesta per il servizio erogato.

I tre livelli sono separati fra loro da appositi sistemi firewall al fine di garantire i migliori livelli di sicurezza:

- Il ***Web Tier*** è il livello dove sono installate le componenti di secure-proxy che permettono di ricevere le richieste provenienti dalla rete internet e di instradarle verso i sistemi applicativi a seguito della corretta autenticazione utente.
- L'***Application Tier*** è il livello dove sono installati i servizi di supporto e di gestione degli utenti.
- Il ***Data Tier*** è il livello dove sono installati gli archivi degli utenti (directory) e quelli di supporto alle applicazioni e ai servizi erogati dalla piattaforma (database).

3.2 Descrizione delle architetture dei sistemi di autenticazione e delle credenziali

Le architetture preposte all'autenticazione degli utenti al SERVIZIO, garamtiscono i due livelli SPID definiti dalle specifiche dell'AGID implementati, ossia il **Livello 1 SPID** e il **Livello 2 SPID**.

Nello specifico:

- ***Livello 1***: è un sistema di autenticazione basato su una ***UserID*** e una ***Password***.

- ***Livello 2***: è un sistema di autenticazione basato su una ***UserID*** e una ***Password***, come già previsto a Livello 1, abbinati ad un codice ***OTP*** [*One-Time Password]* ricevuto via SMS al numero di cellulare dichiarato in fase di Registrazione[1].

I sistemi di autenticazione assicurano inoltre la gestione:

1. **delle autenticazioni per ogni utente;**
2. **del ciclo di vita delle identità;**
3. **della generazione e del mantenimento delle sessioni protette dell'utente.**

A questo scopo, l'architettura è dotata di tre diversi componenti:

1. **Servizi di autenticazione**: hanno la funzione di implementare i flussi di autenticazione e gestire le credenziali necessarie per ogni utente per la verifica l'identità;
2. **Servizi di gestione delle identità**: hanno la funzione di gestire la base dati delle identità e delle differenti credenziali associate ad ogni utente, permettendo il ciclo di vita delle identità (Modifica, Revoca, Sospensione, Riattivazione);
3. **Servizi di federazione**: hanno la funzione di generare i token di autenticazione sulla base delle caratteristiche definite dallo SPID, per le sessione protette.

Nel dettaglio:

- L'applicazione di front-end fornisce all'utente finale l'interfaccia di autenticazione. Tale applicazione utilizza alcune informazioni contenute nell'authnRequest SAML 2.0 emessa dal Service Provider e proveniente tramite redirezione del browser dell'utente, per determinare il livello di autenticazione SPID richiesto. Verrà quindi attivato il flusso di autenticazione opportuno.
- Sulla base del flusso selezionato l'applicazione di front-end interagisce con la componente di autenticazione, per creare una sessione autenticata necessaria ad accedere ai servizi di federazione e con la componente di gestione delle identità digitali per interagire con le credenziali dell'utente. Tale applicazione dispone inoltre delle interfacce necessarie per poter inviare all'utente eventuali SMS o e-mail.
- Il servizio fornisce, all'utente che abbia terminato l'autenticazione con successo e ove consentito dalla normativa, una sessione valida all'accesso ai servizi configurati nella federazione dello SPID. Tale sessione è rappresentata tramite un cookie cifrato salvato sul browser dell'utente.

3.3 Descrizione generale del sistema di monitoraggio

I servizi ed i sistemi gestiti da TI Trust Technologies, sono controllati in modo automatico da due diversi sistemi di monitoraggio che consentono la visualizzazione e la notifica degli allarmi:

- Il "***Sistema Esterno"*** consente il controllo dei servizi erogati in rete dall'infrastruttura effettuando accessi periodici ai servizi tramite collegamento esterno in ADSL su rete internet;
- Il "***Sistema Interno"*** utilizza un Network Management System completamente gestito dagli addetti della CA che consente di mantenere il controllo della rete e dei sistemi fornendo importanti informazioni per la corretta gestione sistemistica.

Le ***principali*** caratteristiche del ***sistema interno*** sono:

- Il controllo del funzionamento dei sistemi in rete;
- Il controllo della raggiungibilità dei sistemi;
- Il controllo dello stato dei sistemi quali ad esempio utilizzo CPU, spazio disco ancora disponibile, corretto funzionamento delle schede di rete, controllo dei processi, ecc.;
- Il controllo del corretto sincronismo dei sistemi rispetto alla sorgente temporale (NTP) tramite l'utilizzo di una fonte esterna (Galileo Ferraris);
- Raccolta e generazione di statistiche sul numero e la tipologia degli allarmi con possibilità di selezionare i singoli apparati o l'intera piattaforma per periodi temporali diversi;

[1] Per aventuali informazioni di dettaglio sui livelli di autenticazione, si rimanda ai paragrafi 6.1 e 6.2 del presente documento.

- Calcolo automatico degli SLA con possibilità di organizzare statistiche per apparati, piattaforme e periodi temporali diversi.

L'esecuzione giornaliera di appositi script segnala tramite Trap al sistema di monitoraggio eventuali modifiche anomale apportate al sistema (es. modifica degli eseguibili, modifica delle utenze).

3.3.1 Monitoraggio sull'utilizzo delle credenziali

Il Gestore garantisce un monitoraggio continuo sull'utilizzo delle credenziali al fine di rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale degli utenti.

Allo scopo si avvale del servizio di autenticazione che offre una protezione completa contro accessi non autorizzati alle risorse mediante l'utilizzo di una combinazione di meccanismi di *strong authentication* e *apposite policy di sicurezza*.

In particolari casi in cui si evidenzi un tentativo, sospetto o meno, di violazione delle credenziali di un utente il Gestore procede alla **sospensione** dell'identità digitale notificando all'utente l'evento rilevato e la necessità di procedere al rinnovo/riemissione delle sue credenziali.

3.4 Descrizione dei codici e dei formati dei messaggi di anomalia

Lo scopo del paragrafo è quello di descrivere, lato utente, i possibili messaggi di errore e le anomalie che potrebbero essere riscontrate. Lo schema seguente mostra il flusso di autenticazione di un utente. Ognuno dei passi descritti dispone di opportune segnalazioni di errore che vengono quindi definite singolarmente nell'ambito della richiesta.

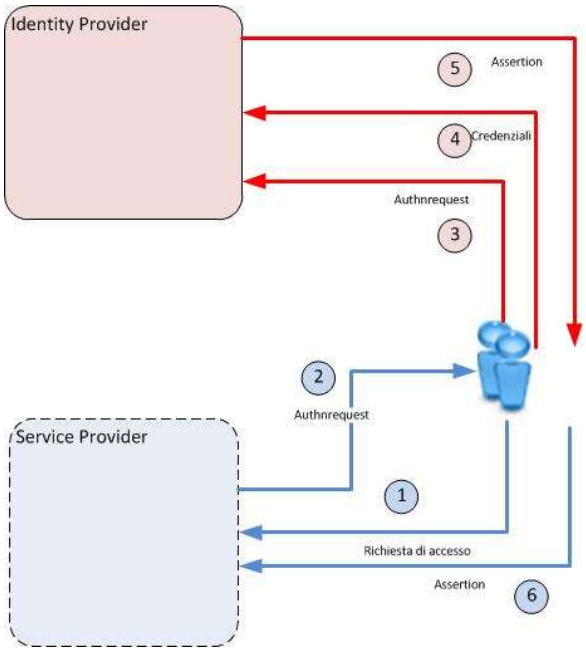

Figura 13 – Flusso di autenticazione utente

3.4.1 Descrizione dei messaggi di errore e anomalia

3.4.1.1 Descrizione dei messaggi di errore sui singoli passi dell'autenticazione

1. L'utente richiede l'accesso ad un servizio erogato da un Service Provider e sceglie l'autenticazione tramite SPID, selezionando il proprio Identity Provider di riferimento.
   (In questa fase, gli eventuali messaggi di errore sono gestiti direttamente dal Service Provider).

2. Il Service Provider genera una richiesta *Authnrequest* SAML 2.0 per l'Identity Provider selezionato e redireziona il browser dell'utente verso di esso.
   (In questa fase, gli eventuali messaggi di errore sono gestiti direttamente dal Service Provider).

3. L'*Authnrequest* viene ricevuta dall'Identity Provider che ne verifica la correttezza e validità.
   I possibili errori in questo caso possono essere:
   a. *Authnrequest* non presente o metodo di invio non conforme a SPID;
   b. *Authnrequest* non valida perché non firmata, malformata o contenente parametri errati o non conformi alle specifiche dello SPID;
   c. *Authnrequest* che non è riconducibile in alcun modo a un Service Provider accreditato SPID;

   In questi casi il Gestore, rilevata la natura dell'anomalia, non può identificare con certezza il Service Provider accreditato e riporta l'esito negativo per l'autenticazione informando direttamente l'utente della natura dell'errore riscontrato mediante una pagina web di cortesia. L'autenticazione non va a buon fine il e Gestore informa l'utente di contattare il Service Provider per l'assistenza.
   d. *Authnrequest* che richiede un livello di autenticazione SPID oppure non disponibile per l'utente presso il Gestore.

   In questi casi il Gestore, rilevata la natura dell'anomalia, emette una *Response* SAML 2.0 firmata che riporta un esito negativo per l'autenticazione, non riporta un'*Assertion* SAML 2.0 ma informa direttamente il Service Provider della natura dell'errore riscontrato. L'autenticazione non va a buon fine e l'utente viene redirezionato automaticametne al servizio del Service Provider senza autenticazione. Il Service Provider indirizzerà l'utente verso l'opportuna procedura in base al tipo di anomalia che si è verificata.

4. Se l'*Authnrequest* è valida, il Gestore mostra all'utente una pagina di autenticazione. In questa pagina viene richiesto l'inserimento dell'identificativo utente (*UserID*) e delle sue credenziali del livello di garanzia richiesto dal Service Provider. In questa pagina viene anche fornita all'utente l'informativa relativa al trattamento dei dati e l'elenco degli attributi della sua Identità Digitale che il Service Provider ha richiesto di ricevere per la transazione.
   I principali errori in questo caso possono essere:
   a. *Identificativo utente non corrispondente ad alcun utente presso il Gestore;*
   b. *Inserimento di credenziali non corrette per il Livello di garanzia SPID richiesto*;
   c. *Inserimento di credenziali relative a una Identità Digitale non attiva (sospesa, revocata, …);*
   d. *Impiego di tempo eccessivo per l'autenticazione rispetto a quanto previsto dal Gestore.*

   In questi casi il Gestore, rilevata la natura dell'anomalia, emette una *Response* SAML 2.0 firmata che riporta un esito negativo per l'autenticazione, non riporta un'*Assertion* SAML 2.0 ma informa il Service Provider della natura dell'errore riscontrato. L'autenticazione non va a buon fine e l'utente viene redirezionato al servizio del Service Provider senza autenticazione. Il Service Provider indirizzerà l'utente verso l'opportuna procedura in base al tipo di anomalia che si è verificata.

5. A fronte di un'autenticazione avvenuta con successo, il Gestore redirige direttamente l'utente verso il servizio del Service Provider, trasferendogli una *Response* SAML 2.0 firmata che riporta il successo dell'autenticazione. La *Response* SAML 2.0 contiene un'*Assertion* SAML 2.0 firmata dal Gestore con gli attributi dell'Identità Digitale dell'utente richiesti dal Service Providers e previsti nella configurazione SPID del Service Provider (Metadata di SP).
   Nel caso di problemi nell'elaborazione dell'autenticazione da parte del Gestore, l'utente viene rediretto su una apposita pagina di cortesia erogata dal Gestore che lo informa della natura del problema e su come procedere di conseguenza.

6. Se l'autenticazione procede correttamente, la *Response* SAML 2.0 viene quindi restituita dal Gestore al browser dell'utente che viene rediretto al Service Provider.
   (Gli eventuali messaggi di errore relativi alla elaborazione della *Response* SAML 2.0 e dell'*Assertion* SAML 2.0 da parte del Service Provider sono gestiti direttamente dal Service Provider stesso).

La *Response* SAML 2.0 emessa e firmata dal Gestore contiene sempre al suo interno un campo *Status* che, nei sottocampi *StatusCode e StatusMessage,* riporta il risultato dell'operazione di autenticazione, in particolare:

- Se *StatusCode* è impostato al valore *urn:oasis:names:tc:SAML:2.0:status:Success* l'autenticazione dell'Identità Digitale è terminata con successo e il campo *Assertion* contiene gli attributi da trasmessi al Service Provider.
- Se *StatusCode* contiene il valore *urn:oasis:names:tc:SAML:2.0:status:Requester*, significa che il Gestore ha rilevato un'anomalia o un errore riferibile alla richiesta di autenticazione inviata dal Service Provider e non ha potuto concludere l'operazione. E' previsto che un ulteriore *StatusCode* e uno *StatusMessage* riportino il dettaglio dell'anomalia.
- Se *StatusCode* contiene il valore *urn:oasis:names:tc:SAML:2.0:status:Responder*, significa che il Gestore non ha potuto completare l'operazione di autenticazione per un motivo riferibile all'utente oppure a altro motivo relativo al proprio servizio. Anche in questo caso è previsto che un ulteriore *StatusCode* e uno *StatusMessage* riportino il dettaglio dell'anomalia.

3.4.1.2 Messaggi relativi ai meccanismi di autenticazione

Durante l'autenticazione dell'Identità Digitale l'utente interagisce direttamente col servizio del Gestore e poi viene reindirizzato al servizio del Service Provider che aveva originalmente chiesto di utilizzare.

I sistemi di autenticazione predisposti dal Gestore consistono nelle cosiddette "credenziali" delle quali l'utente deve garantire la riservatezza per la tutta la durata dell'Identità Digitale.

Il servizio del Gestore prevede dei messaggi di informazione o di anomalia che vengono mostrati all'utente nelle differenti situazioni che si possono verificare durante il processo di autenticazione.

Nel caso del livello di garanzia L1 SPID, basato per il Gestore sull'utilizzo di una UserID e una Password, è previsto che siano mostrate delle segnalazioni all'utente nei seguenti casi:

- Mancato inserimento di un dato obbligatorio (es. UserID o Password)
- Inserimento di valori errati per le credenziali (es. UserID o Password)
- Superamento del numero massimo di inserimenti di valori errati per le credenziali.

Nel caso del livello di garanzia L2 SPID, basato per il Gestore sull'utilizzo di una UserID e una Password, e su un codice OTP inviato tramite SMS, è previsto che siano mostrate delle segnalazioni nei seguenti casi:

- Mancato inserimento di un dato obbligatorio (es. UserID, Password, OTP, …)
- Inserimento di valori errati per le credenziali (es. UserID, Password, OTP, …)
- Superamento del numero massimo di inserimenti di valori errati per le credenziali.

La Guida Utente del servizio del Gestore riporta tutte le informazioni e le istruzioni per l'utilizzo corretto del servizio.

3.5 Descrizione generale delle misure anticontraffazione

Il concetto generale di contraffazione comporta una valutazione di confondibilità dell'oggetto contraffatto con quello genuino; nella legislazione il termine contraffazione è associato spesso a reati legati alla violazione di marchi o brevetti, monete o banconote, certificati o documenti, merci.

Nell'ambito specifico del SERVIZIO, le regole e le policy di sicurezza da adottare al fine di garantire un contesto di autenticazione affidabile sono definite dalla norma ISO/IEC 29115 che, in base all'art.6 del DPCM 24/10/2014, il Gestore deve soddisfare relativamente ai livelli di sicurezza delle Identità Digitali. La norma colloca il rischio specifico della contraffazione in due precisi ambiti:

1. Processo di Identificazione e verifica dell'Identità del Richiedente l'Identità Digitale ("*8.1.2 Identity proofing and identity information verification* "): la verifica dell'identità può includere il controllo fisico dei documenti di identità presentati per individuare possibili frodi, manomissioni o contraffazioni ("I*dentity proofing may include the physical checking of presented identity documents to detect possible fraud, tampering, or counterfeiting*");
2. Controlli di sicurezza anticontraffazione (*AntiCounterfeiting*) richiesti al fine di mitigare la duplicazione delle credenziali (*CredentialDuplication*) durante l'utilizzo delle credenziali di autenticazione; la credenziale dell'utente viene illegittimamente copiata: misure anti-contraffazione devono essere adottate sui dispositivi che custodiscono le credenziali.

Nel primo ambito (1), nella fase di Identificazione del Richiedente, le misure adottate dal Gestore per mitigare il rischio di contraffazione sono:

- la *Procedura di Identificazione a vista*, nelle modalità '*de-visu*' e 'tramite sistemi di *registrazione Audio-Video*' (da remoto); in questo caso il Gestore, verifica che il volto del richiedente corrisponda a quello presente sulle fotografie riportate sui documenti di identità presentati.
- la Procedura di identificazione tramite *firma elettronica qualificata* o *firma digitale* apposta sul modulo di richiesta; in questo caso il Gestore considera che la fase di identificazione del Richiedente sia stata correttamente espletata dal Certificatore che ha emesso il certificato qualificato utilizzato per apporre la firma al modulo di richiesta;
- la Procedura di identificazione tramite *CNS o CIE*; in questo caso il Gestore considera che la fase di identificazione del Richiedente sia stata correttamente espletata dal Certificatore che ha emesso il certificato CNS o CIE utilizzato per produrre *attestazione*[2] del modulo di richiesta;

A seguito di tutte le procedure di identificazione il Gestore esegue, ove disponibili, le verifiche dei dati identificativi dichiarati dal Richiedente tramite fonti autoritative esterne, come prescritto dalla norma (all'art.4 comma 1 lettera c) del DPCM 24/10/2014).

Nel secondo ambito (2), si possono distinguere due fasi distinte nelle quali il Gestore applica le misure necessarie a mitigare il rischio:

- Consegna delle credenziali: il processo di consegna delle credenziali prevede l'uso di due diversi canali (e-mail + SMS) per l'utilizzo della password di primo accesso e l'impostazione della password personale;

- Gestione delle credenziali:
  - da parte del Gestore: i sistemi che custodiscono le credenziali (*LoA2 Password*) non sono accessibili in nessun caso dall'esterno, in aggiunta l'accesso logico a tali sistemi (repository) è consentito solo agli Amministratori di Sistema – nominati ed autorizzati direttamente dal Responsabile della Sicurezza del Gestore; al Livello 2, il secondo fattore della credenziale è costituito da un "*token out-of-band*" di Livello 1 (*OTP ricevuto via SMS* al numero di telefono cellulare del titolare), in tal modo non sono necessarie ulteriori misure anti-contraffazione di quelle previste al Livello 1;
  - da parte dell'Utente: nella Guida Utente del servizio, particolare attenzione viene data dal Gestore nel descrivere all'Utente le modalità raccomandate per la tenuta e la gestione delle credenziali e degli strumenti ad esse associati (ad esempio, non mantenere mai l'Identificativo Utente e la password scritte da qualche parte; durante una sessione autenticata non lasciare la postazione incustodita e sbloccata; mantenere sempre il controllo del proprio telefono cellulare; ecc.).

Uno studio sulle ulteriori minacce (e le relative misure adottate) correlate alla contraffazione è descritto nel documento di Analisi del rischio del Gestore.

3.6 Livelli di servizio garantiti

In coerenza con la normativa di riferimento dello SPID, il Gestore si impegna a garantire i livelli di servizio secondo gli Indicatori di Qualità che sono riassunti nella tabella seguente e che devono essere misurati e calcolati su base trimestrale secondo le modalità riportate nella *Convenzione IDP SPID*.

Il Gestore pubblica la propria Carta dei Servizi al link: https://www.trusttechnologies.it/SPID.

Nella normativa gli Indicatori di Qualità sono definiti in relazione ai principali sottoservizi erogati dal Gestore e che sono stati definiti come:

- Attivazione dell'Identità Digitale, suddivisa nelle fasi:
  - Registrazione dell'Identità Digitale
  - Rilascio delle Credenziali
- Gestione del Ciclo di Vita dell'Identità Digitale:
  - Sospensione/Riattivazione/Revoca dell'Identità Digitale
  - Rinnovo delle credenziali relative all'Identità Digitale

[2] Per *Attestazione* si intende la firma elettronica di un documento effettuata con chiave privata e certificato di autenticazione a bordo della CNS o della CIE.

- Servizio di Autenticazione online dell'Identità Digitale

Durante il normale funzionamento, per ogni sottoservizio è prevista la rilevazione dei livelli diservizio erogati dal Gestore secondo due Indicatori di Qualità:

- uno relativo alla *Disponibilità* del sottoservizio ossia alla sua effettiva fruibilità da parte dell'utilizzatore in termini temporali (es. ore, giorni, …);
- uno relativo al *Tempo di Risposta* del sottoservizio ossia al massimo tempo che il Gestore impiega per completare, per le componenti di sua competenza del processo, quanto previsto dal sottoservizio stesso una volta che ha a disposizione tutto il necessario.

Gli Indicatori sono stati definiti inoltre tenendo conto che alcuni sottoservizi possono essere erogati dal Gestore in modalità differenti, in particolare mediante sistemi automatici (es. sistema web online) piuttosto che con la presenza fisica di un operatore del Gestore (es. presso uno sportello del Gestore oppure con un operatore in sede del Gestore).

ID	Indicatore di Qualità	Modalità di funzionamento	Valore Limite
IQ-01	Disponibilità del sottoservizio di Registrazione Identità Digitale	*Erogazione automatica*	>= 99,0% con singolo evento di indisponibilità <= 6 ore
		Erogazione in presenza	>= 98,0%
IQ-02	Tempo di Risposta del sottoservizio di Registrazione Identità Digitale		<= 24 ore lavorative
IQ-03	Disponibilità del sottoservizio di Rilascio Credenziali	*Erogazione automatica*	>= 99,0% con singolo evento di indisponibilità <= 6 ore
		Erogazione in presenza	>= 98,0%
IQ-04	Tempo di Rilascio Credenziali		<= 5 giorni lavorativi
IQ-05	Tempo Riattivazione delle Credenziali		<= 2 giorni lavorativi
IQ-06	Disponibilità del sottoservizio di Sospensione e Revoca delle Credenziali		>= 99,0% con singolo evento di indisponibilità <= 6 ore
IQ-07	Tempo di Sospensione delle Credenziali		<= 30 minuti
IQ-08	Tempo di Revoca delle Credenziali		<= 5 giorni lavorativi
IQ-09	Disponibilità del sottoservizio di Rinnovo e Sostituzione delle Credenziali	*Erogazione automatica*	>= 99,0%
		Erogazione in presenza	>= 98,0%
IQ-10	Tempo di Rinnovo e Sostituzione delle Credenziali		<= 5 giorni lavorativi

IQ-11	Disponibilità del sottoservizio di Autenticazione		>= 99,0% con singolo evento indisponibilità <= 4 ore
IQ-12	Tempo di risposta del sottoservizio di Autenticazione (per le sole componenti di elaborazione in carico al Gestore)		<=3 sec almeno per il 95,0% delle richieste ricevute

I servizi del Gestore sono erogati in coerenza con i più moderni standard di Business Continuity per i servizi ICT e in linea con la normativa. In caso di grave anomalia (disastro) è prevista l'attivazione di un servizio di emergenza denominato di Disaster Recovery.

Per l'attivazione del servizio di emergenza il Gestore si impegna a garantire il rispetto degli specifici Indicatori di Qualità previsti dalla normativa e definiti come:

- *Recovery Time Objective* o RTO: Obbiettivo temporale di ripristino del servizio ossia il tempo massimo che il Gestore impiega, in caso di Disastro, per attivare un servizio di emergenza alternativo;
- *Recovery Point Objective* o RPO: Massima perdita (in termini di tempo) di dati elaborati prima del Disastro che è ammissibile non riuscire a recuperare all'attivazione del servizio di emergenza alternativo.

ID	Indicatore di Qualità	Valore Limite
IQ-13	RPO sottoservizi di Registrazione e di Rilascio delle Identità Digitali	1 ora
IQ-14	RTO sottoservizi di Registrazione e di Rilascio delle Identità Digitali	8 ore
IQ-15	RPO sottoservizio di Sospensione e Revoca delle Credenziali	1 ora
IQ-16	RTO sottoservizio di Sospensione e Revoca delle Credenziali	8 ore
IQ-17	RPO sottoservizio di Autenticazione	1 ora
IQ-18	RTO sottoservizio di Autenticazione	8 ore

Il Gestore, oltre a quanto sopra riportato, si impegna a garantire l'integrità e la disponibilità delle tracciature relative alle transazioni di autenticazione già concluse, anche a seguito di un evento di Disaster Recovery.

Il titolare di una Identità Digitale può visualizzare direttamente i contenuti del registro delle transazioni di autenticazione ad essa relative collegandosi al Portale del Gestore. Eventuali richieste al di fuori dei termini previsti dal Portale e relative alle transazioni degli ultimi 24 mesi possono essere richieste dal titolare a mezzo di documento cartaceo inviato per raccomandata A/R o a mezzo di documento informatico (firmato con firma elettronica qualificata o con firma digitale) invato per Posta Elettronica Certificata.

4 Modello Operativo del Servizio

4.1 Descrizione del Servizio

La **descrizione del servizio,** la **Guida Utente** e la **Carta dei Servizi** sono documenti direttamente disponibili per la consultazione e per il download al seguente indirizzo internet: http://www.trusttechnologies.it/SPID.

Il **Sistema Pubblico per la gestione dell'Identità Digitale** di cittadini e imprese (**SPID**) è costituito (ai sensi del comma 2-ter dell'art. 64 del [CAD]) come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite nel [DPCM SPID], gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni o dei soggetti privati che aderiranno al sistema, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.

Il sistema SPID ha lo scopo principale di definire un ambiente sicuro, efficace ed economico per consentire l'accesso, per i cittadini e le imprese, ai servizi offerti da tutte le amministrazioni pubbliche (e dai fornitori di servizi aderenti al sistema) in modalità telematica in coerenza con una strategia che privilegia il digitale per default.

Il modello segue un approccio federato per la fornitura dei servizi di identità digitale in modo da:

- consentire ai cittadini e alle imprese di scegliere autonomamente il gestore delle identità digitale certificato, e
- creare un mercato libero e competitivo che stimoli una concorrenza virtuosa ed un continuo miglioramento delle soluzioni tecnologiche e dei sistemi.

Il modello SPID prevede la separazione delle funzioni di identificazione (di competenza dei gestori dell'identità digitale) dalle funzioni di attestazione e autenticazione degli attributi qualificati (di competenza dei gestori di attributi qualificati).

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** (**corrispondente al livello LoA2 dell'ISO-IEC 29115**) prevede sistemi di autenticazione a singolo fattore, ad es. la password; questo livello può essere considerato adeguato nei casi in cui il danno causato, da un utilizzo indebito dell'identità digitale, ha un basso impatto per le attività del cittadino/impresa/amministrazione;
- **Livello 2** (**corrispondente al livello LoA3 dell'ISO-IEC 29115**) prevede un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali; questo livello è adeguato per tutti i servizi che possono subire un danno consistente da un utilizzo indebito dell'identità digitale;
- **Livello 3** (**corrispondente al livello LoA4 dell'ISO-IEC 29115**) 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; questo è il livello di garanzia più elevato e da associare a quei servizi che possono subire un serio e grave danno per cause imputabili ad abusi di identità.

Il servizio erogato dal Gestore prevede la fornitura dell'autenticazione SPID di Livello 1 e Livello 2, non prevede il Livello 3.

4.2 Schema di gestione delle identità digitali

4.2.1 Persone fisiche

Per le persone fisiche, il servizio erogato prevede la fornitura delle Identità Digitali del **Tipo 1**, secondo la definizione presente nell'Avviso SPID n. 18 v2. Non è disponibile la fornitura delle Identità Digitali per Uso Professionale per persone fisiche (**Tipo 3).**

A ogni persona fisica viene assegnata, nel sistema del Gestore, una identità univoca caratterizzata dagli attributi identificativi previsti dalla normativa SPID (nome, cognome, luogo e data di nascita, sesso) e alla quale viene assegnato un codice univoco interno. Questa identità viene inserita nel sistema in occasione dell'attivazione del servizio per la persona oppure, come predisposizione, in caso di migrazione dei dati da altro Service Provider.

Quando una persona richiede l'attivazione della propria identità digitale, alla sua identità univoca viene associata una identità digitale. L'identità digitale è caratterizzata da attributi "identificativi" e "non identificativi", dal riferimento al *Service Provider* a cui la richiesta di attivazione afferisce ed alle credenziali che vengono attivate e consegnate alla persona.

Quando un Service Provider richiede una identità digitale per una persona fisica essa viene attivata ed associata al richiedente.

4.2.2 Persone giuridiche

Per le persone giuridiche, il servizio erogato prevede la fornitura delle Identità Digitali del **Tipo 2**, secondo la definizione presente nell'Avviso SPID n. 18 v2. Non è disponibile la fornitura delle Identità Digitali per Uso Professionale per persone giuridiche (**Tipo 4).**

A ogni persona giuridica viene assegnata, nel sistema del Gestore, una identità univoca caratterizzata dagli attributi identificativi previsti dalla normativa SPID e alla quale viene assegnato un codice SPID.

Ad essa è associata una identità di persona fisica – corrispondente all'amministratore o legale rappresentante – con un proprio codice SPID.

4.3 Processi del servizio

I processi operativi del Gestore si articolano come segue:

- **Attivazione del servizio**
  - Obblighi del Gestore e del Titolare
  - Modalità di interazione Gestore - Utente

- **Registrazione utente**
  - Pre-registrazione (*Richiesta*)
  - Identificazione (*Dimostrazione e Verifica delle informazioni di identità*)
  - Creazione identità digitale

- **Gestione delle credenziali**
  - Emissione delle credenziali
  - Consegna delle credenziali

- **Autenticazione**
  - Gestione delle richieste di autenticazione
  - Meccanismi di autenticazione

- **Registro delle attività**
  - Conservazione dei documenti previsti dalla normativa per la registrazione delle identità

- **Gestione del ciclo di vita dell'Identità Digitale**
  - Visualizzazione attività
  - Modifica (attributi, credenziali)
  - Revoca
  - Sospensione
  - Riattivazione

5 Attivazione del SERVIZIO

L'attivazione del SERVIZIO può avvenire in 2 modalità:

1. Attivazione sulla base di specifici accordi bilaterali, secondo le disposizioni del **[Regolamento Identità Pregresse]** ;
2. Attivazione diretta tramite le modalità previste dal servizio.

5.1 Modalità di interazione con l'utente

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

CANALI	
TIM Digital Store **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 di emergenza 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 **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. Durante la procedura 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 Nel caso l'utente abbia richiesto l'identificazione con firma elettronica qualificata o digitale oppure con CNS o CIE 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 E-MAIL
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.

Sito istituzionale di TIM e di TIM Digital Store	Sul sito di TIM, i Clienti trovano le informazioni relative all'offerta ed i necessari rimandi al sito di Trust Technologies e alle specifiche sezioni relative a TIMid.

6 Registrazione dell'Identità Digitale

La **Registrazione** è il processo in cui un soggetto (persona fisica o giuridica) chiede al Gestore di attivare la propria identità digitale.

La fase di Registrazione si compone, per il Gestore, dei seguenti processi:

1. *Pre-registrazione (richiesta e adesione)*;
2. *Identificazione*;
3. *Verifica delle informazioni d'identità*.

Questi processi possono essere condotti interamente da una singola organizzazione o da più organizzazioni.

6.1 Pre-registrazione (richiesta e adesione)

La fase di pre-registrazione si avvia con la **richiesta** presentata dal soggetto persona fisica o persona giuridica per ottenere l'identità digitale.

La fase di **pre-registrazione per soggetti persone fisiche** è resa possibile dal Gestore in due modalità:

- effettuata online dal Richiedente;
- effettuata dal Richiedente recandosi direttamente presso un negozio TIM abilitato, con l'intervento di un incaricato del Gestore.

Di seguito si riporta graficamente il flusso di pre-registrazione effettuata online dal Richiedente, valido sia nel caso di richiesta avanzata da persona fisica o persona giuridica:

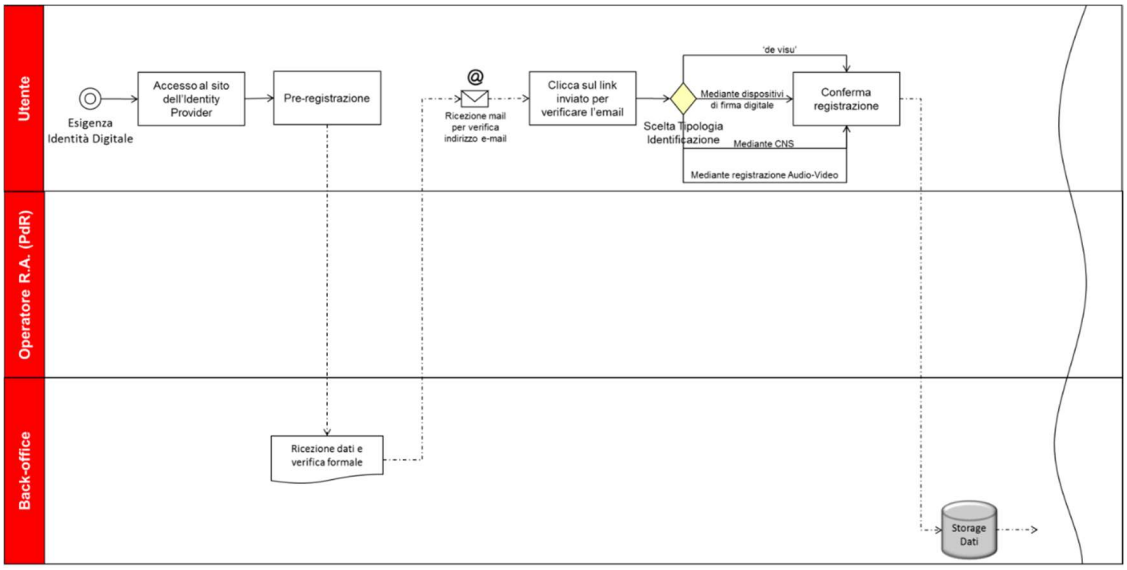

Figura 24 - Flusso di Pre-registrazione effettuata online dal Richiedente

Di seguito si riporta il flusso con il quale il Richiedente effettua la pre-registrazione recandosi direttamente presso un negozio TIM abilitato:

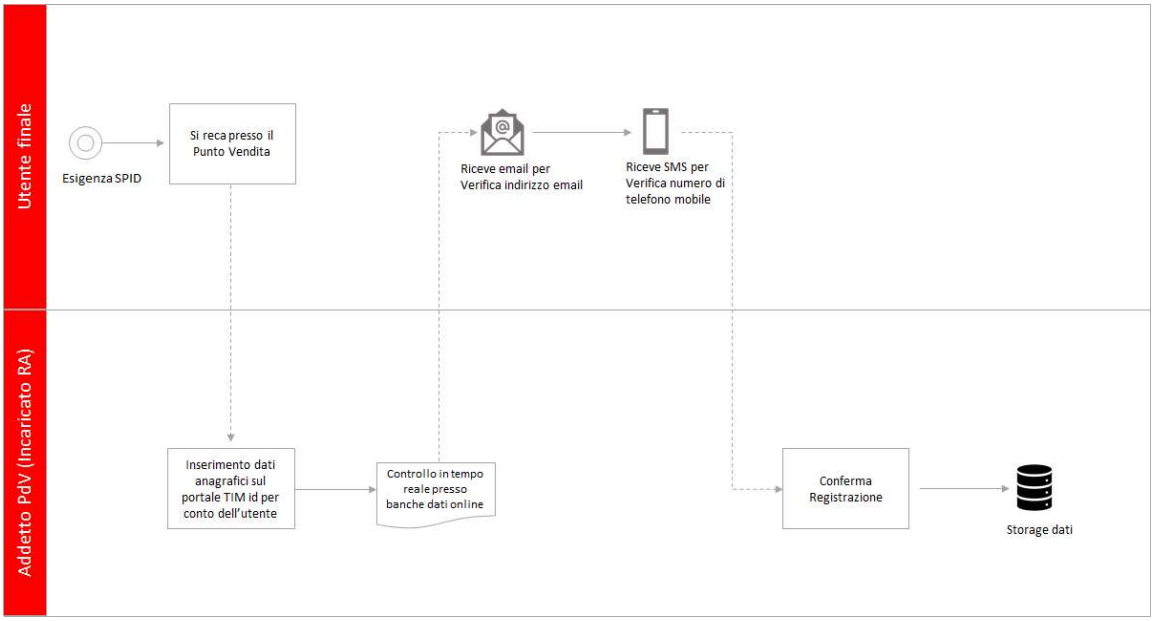

Figura 5 - Flusso di Pre-registrazione effettuata dal Richiedente presso il Negozio TIM

6.1.1 Persona fisica

La fase di pre-registrazione per soggetti persone fisiche inizia con la compilazione di un *Modulo di Richiesta (application form)* attraverso il Portale di Gestione del servizio di Identità Digitale erogato dal Gestore. Questo modulo deve registrare informazioni sufficienti per garantire che il soggetto possa essere univocamente identificato all'interno dello SPID.

In particolari condizioni, che dipendono dal canale utilizzato dal Richiedente per l'attivazione del SERVIZIO, il Richiedente non compila direttamente il *Modulo di Richiesta* ma conferma alcuni dati precaricati non modificabili e aggiorna/completa i soli dati modificabili.

Nel caso del negozio TIM il Richiedente riferisce i propri dati a un incaricato del Gestore che compila la richiesta per suo conto.

Questa fase è composta dai seguenti passi eseguiti in sequenza dal Richiedente oppure dall'incaricato del negozio TIM.

6.1.1.1 Richiesta

- Il Richiedente si collega online via web all'apposita sezione di *pre-registrazione* sul Portale dei Servizi di Identità Digitale (o Portale) predisposto dal Gestore oppure si reca presso il negozio TIM abiliato;
- Il Portale propone al Richiedente (o all'incaricato del negozio TIM) una *form* all'interno della quale deve compilare almeno i seguenti campi (obbligatori):

Attributi Identificativi	Attributi Secondari
Nome e Cognome	Estremi di un documento di Identità *(Numero, Tipo, Emettitore, Data scadenza)*
Sesso	Numero di telefono cellulare *(dichiarato dal Richiedente)*
Data e luogo di nascita	E-mail *(dichiarato dal Richiedente)*

Codice Fiscale	Indirizzo di Domicilio
User ID	Numero della Tessera Sanitaria

- Il Portale effettua verifiche formali sui dati inseriti dal Richiedente e procede al salvataggio dei dati generando un *Codice di Registrazione* personale che identifica univocamente la richiesta.
- Durante questa fase viene anche verificato, mdiante l'invio di appositi codici segreti, che il Richiedente abbia il controllo effettivo della casella di posta elettronica e del numero di telefono cellulare dichiarati.

6.1.1.2 Adesione

Nel caso della richiesta effettuata online, il Portale propone al Richiedente la scelta della modalità di Identificazione desiderata tra quelle disponibili:

- "di persona", mediante esibizione 'a vista' di un documento di identità ("de-visu") presso una delle sedi messe a disposizione dal Gestore sulla base di appositi accordi.
- "informatica", mediante utilizzo della propria firma elettronica qualificata per sottoscrivere la richiesta di adesione da remoto,
- "informatica", mediante utilizzo della propria carta CNS o della propria CIE per attestare la richiesta di adesione da remoto,
- "di persona, da remoto", mediante sistemi di registrazione Audio-Video;

Nel caso della richiesta effettuata presso il negozio TIM, è prevista esclusivamente la modalità di Identificazione:

- "di persona", mediante esibizione 'a vista' di un documento di identità ("de-visu");

Il Richiedente riceve dal Portale la conferma tramite e-mail contenente i dati riepilogativi di registrazione ed il *Codice di Registrazione*, con le istruzioni da utilizzare nella fase successiva di Identificazione.

6.1.2 Persona giuridica

La fase di pre-registrazione è iniziata come **richiesta** presentata dal soggetto persona giuridica per ottenere una identità digitale.

Il processo di avvio della fase di pre-registrazione per soggetti persone giuridiche prevede la compilazione, da parte di una persona fisica rappresentante (il Richiedente, nel seguito) della persona giuridica, di un *Modulo di Richiesta (application form)* attraverso il Portale di Gestione del servizio di Identità Digitale. Questo modulo deve registrare informazioni sufficienti per garantire che il soggetto possa essere univocamente identificato all'interno di un contesto.

In particolari condizioni, che dipendono dal canale utilizzato dal Richiedente per l'attivazione del SERVIZIO, il Richiedente non compila direttamente il *Modulo di Richiesta* ma conferma alcuni dati precaricati non modificabili e aggiorna/completa i soli dati modificabili.

Questa fase è composta dai seguenti passi eseguiti in sequenza dal Richiedente, in modalità remota.

6.1.2.1 Richiesta

- Il Richiedente si collega online via web all'apposita sezione di *pre-registrazione* sul Portale dei Servizi di Identità Digitale (o Portale) predisposto dal Gestore;
- Il Portale propone al Richiedente una *form* all'interno della quale deve compilare almeno i seguenti campi (obbligatori):

Attributi identità digitale	Attributi Secondari identità digitale
UserID SPID	Numero di telefono mobile usato per l'autenticazione SPID
Attributi identità azienda	**Attributi Secondari azienda**
Denominazione/Ragione sociale	Sede legale
Codice Fiscale o Partita IVA *(se uguale al Codice Fiscale)*	
Attributi rappresentante legale	
Nome e Cognome	Indirizzo E-mail
	Domicilio fisico
Estremi documento d'identità (Numero, Tipo, Emettitore, Data scadenza)	Numero tessera sanitaria
Certificazione 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)	

- Il Portale effettua verifiche formali sui dati inseriti dal Richiedente e procede al salvataggio degli stessi generando un *Codice di Registrazione* personale che il Richiedente potrà utilizzare, insieme al Codice Fiscale, per completare la procedura di Registrazione; infine invia al Richiedente una e-mail contenente un link – con validità limitata nel tempo – per confermare la richiesta di adesione;

6.1.2.2 Adesione

- Il Richiedente conferma la richiesta di adesione tramite il link ricevuto all'indirizzo e-mail dichiarato in fase di Registrazione (questo passo può essere eseguito anche in un secondo momento e comunque entro la scadenza del link di conferma);
- Il Portale convalida la richiesta e propone al Richiedente la scelta della modalità di Identificazione desiderata tra quelle disponibili:
  - *"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 o della propria CIE per attestare la richiesta di adesione da remoto,
  - "*di persona, da remoto*", mediante sistemi di registrazione Audio-Video;
- Il Richiedente effettua la scelta della modalità di Identificazione desiderata e, per la modalità di identificazione *"di persona"* ('*de-visu*'), effettua anche l'upload delle immagini fronte/retro del documento di identità e della Tessera Sanitaria (come evidenza del Codice Fiscale) e del documento di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del richiedente l'identità digitale per conto della persona giuridica (*Visura Camerale* firmata dalla CCIAA o, in alternativa, *Copia dell'Atto notarile di Procura legale* firmata digitalmente dal Richiedente). Il Richiedente riceve dal Portale la conferma tramite e-mail contenente i dati riepilogativi di registrazione ed il *Codice di Registrazione*, con le istruzioni da utilizzare nella fase successiva di Identificazione.

6.2 Identificazione (dimostrazione e verifica dell'identità)

L'**Identificazione** *(Identity proofing)* è il processo di acquisizione delle informazioni sufficienti per identificare un soggetto ad un livello di garanzia specificato.

La *dimostrazione dell'identità* 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.

La *verifica dell'identità* consiste invece nel controllo delle informazioni confrontando i dati forniti con informazioni precedentemente convalidate ed il legame con il soggetto richiedente.

Sia il processo di dimostrazione dell'identità che il processo di verifica sono eseguiti allo scopo di ottenere un garantito livello di sicurezza dell'identità del soggetto richiedente prima di completare la registrazione.

Nel seguito sono descritte le modalità di identificazione che il Gestore TI Trust Technologies ha previsto, nel caso di soggetto persona fisica e soggetto persona giuridica.

6.2.1 Persona fisica

6.2.1.1 Identificazione mediante esibizione 'a vista' di un documento di identità ('de visu') presso una sede delegata del Gestore

In questa modalità di identificazione il Richiedente si reca presso il Punto di Registrazione (PdR) e viene identificato 'de visu' ossia di persona tramite esibizione a vista di un valido documento d'identità.

Questa modalità è composta dai seguenti passi eseguiti in sequenza, prima dal personale di Back-Office presso il Gestore, poi dal Richiedente e dall'Incaricato (dal Gestore) presso il PdR.

6.2.1.1.1 Verifiche documentali (back office) e provisioning certificato di FEA

1. Presso il Gestore il personale di Back-Office procede alle verifiche documentali ovvero delle informazioni presenti nella Scheda di Registrazione mediante:
   a. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni (cfr.3.5),
   b. eventuali controlli manuali su fonti autoritative[3] in sostituzione dei controlli automatici (cfr.3.5);
2. Al termine delle verifiche il Back-Office convalida la richiesta ed il sistema del Gestore avvia il provisioning del Certificato di FEA associato al Richiedente (effettuato invocando dei web services esposti dalla Piattaforma di Firma Remota Qualificata del Certificatore Trust Technologies). Il Certificato di FEA è emesso da una Certification Authority non accreditata e verrà utilizzato per firmare la documentazione contrattuale del Richiedente con il Gestore;

6.2.1.1.2 Dimostrazione dell'identità

3. Presso il PdR il Richiedente presenta il proprio *Codice di Registrazione* ottenuto alla conferma della pre-registrazione;
4. L'Incaricato presso il PdR accede al Portale dei Servizi di Identità Digitale con le proprie credenziali, inserisce il *Codice di Registrazione* presentato dal Richiedente e richiama a video la Scheda di Registrazione con i relativi dati anagrafici;
5. Il Richiedente presenta un documento di identità in corso di validità e la propria Tessera Sanitaria (come evidenza del Codice Fiscale);

6.2.1.1.3 Verifica dell'identità (front office)

6. L'Incaricato presso il PdR procede alla verifica dell'identità ovvero verifica la corrispondenza tra documenti identificativi presentati e presenza fisica del richiedente ('de-visu');

[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.

7. L'Incaricato presso il PdR richiama a video il *Modulo di Adesione* precompilato con i dati anagrafici validati dal Richiedente in fase di pre-registrazione, contenente anche le Condizioni Generali di Utilizzo del servizio di Identità Digitale e l'Informativa Privacy sul trattamento dei dati personali che vengono confermate dal Richiedente tramite apposizione firma FEA. L'Incaricato presso il PdR avvia la verifica del numero di cellulare, dichiarato dal Richiedente in fase di registrazione, ed avvia il processo di firma FEA del *Modulo di Adesione* tramite OTP;
8. Il Richiedente comunica all'Incaricato presso il PdR il codice OTP ricevuto via SMS che viene utilizzato per convalidare i dati identificati e per firmare digitalmente il *Modulo di Adesione*;
9. L'Incaricato presso il PdR inserisce il codice OTP sul Portale dei Servizi di Identità Digitale. Il codice OTP inserito è quello che il Richiedente ha ricevuto via SMS al numero di telefono cellulare, dichiarato dal Richiedente in fase di registrazione. Il sistema del Gestore elabora la richiesta, appone la firma FEA (effettuata invocando dei web services esposti dalla Piattaforma di Firma Remota Qualificata del Certificatore Trust Technologies) al *Modulo di Adesione*;
10. L'Incaricato presso il PdR riceve conferma dal Portale dei Servizi di Identità Digitale del Gestore del completamento della richiesta e del salvataggio nell'area di 'Self-Customer Care' del Richiedente della documentazione prodotta (Modulo di Adesione, Condizioni Generali di Utilizzo e Informativa Privacy);
11. Il Richiedente riceve conferma via e-mail dell'avvenuta emissione delle credenziali e della disponibilità, nella propria area di 'Self-Customer Care' e per tutto il periodo contrattuale, della documentazione sottoscritta digitalmente (Modulo di Adesione, Condizioni Generali di Utilizzo e Informativa Privacy).

Di seguito un diagramma che rappresenta il flusso sopra descritto:

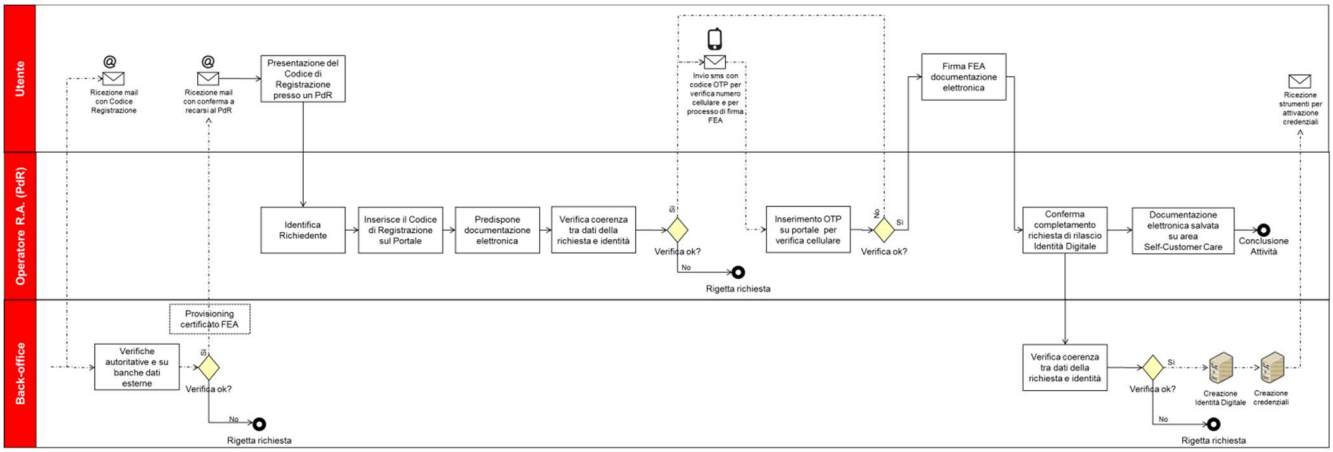

Figura 6 - Flusso di rilascio Identità Digitale per persona fisica con identificazione 'De Visu' presso una sede delegata dal Gestore

6.2.1.2 Identificazione mediante esibizione 'a vista' di un documento di identità ('de visu') presso un negozio TIM

In questa modalità di identificazione il Richiedente si reca presso uno dei negozi TIM abilitati e viene identificato 'de visu' ossia di persona dal personale incaricato del negozio tramite esibizione a vista di un valido documento d'identità.

Questa modalità è composta dai seguenti passi eseguiti dal Richiedente e dal personale incaricato dal Gestore presso il Negozio.

6.2.1.2.1 Verifiche documentali e provisioning certificato di FEA

1. A Seguito della fase di pre-registrazione effettuata dall'incaricato del negozio assieme al Richiedente (descritta al par. xxx) il servizio di registrazione del Gestore procede alle verifiche documentali ovvero delle informazioni presenti nella Scheda di Registrazione mediante:
    a. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni (cfr.3.5),

b. eventuali controlli manuali su fonti autoritative[4] in sostituzione dei controlli automatici (cfr.3.5);

2. Al termine delle verifiche l'incaricato del negozio TIM convalida la richiesta ed il sistema del Gestore avvia il provisioning del Certificato di FEA associato al Richiedente (effettuato invocando dei web services esposti dalla Piattaforma di Firma Remota Avanzata del Certificatore Trust Technologies). Il Certificato di FEA è emesso da una Certification Authority non accreditata e viene utilizzato per firmare la documentazione contrattuale del Richiedente con il Gestore;

6.2.1.2.2 Dimostrazione dell'identità

3. Il Richiedente presenta un documento di identità in corso di validità e la propria Tessera Sanitaria (come evidenza del Codice Fiscale);
4. L'Incaricato del negozio verifica i documenti presentati dal Richiedente;

6.2.1.2.3 Verifica dell'identità

5. L'Incaricato presso il negozio TIM procede alla verifica dell'identità ovvero verifica la corrispondenza tra documenti identificativi presentati e presenza fisica del richiedente ('de-visu');
6. L'Incaricato presso il negozio TIM carica a sistema le fotografie fronte e retro del documento d'identità e della tessera sanittaria del Richiedente.
7. A seguito della verifica positiva sulle banche dati autotirtative, l'Incaricato avvia il processo di firma FEA del *Modulo di Adesione* da parte del Richiedente, tramite OTP via SMS;
8. Il Richiedente comunica all'Incaricato del negozio TIM il codice OTP ricevuto via SMS;
9. L'Incaricato del negozio TIM inserisce il codice OTP riferito dal Richiedente, sul Portale dei Servizi di Identità Digitale. Il codice OTP inserito è quello che il Richiedente ha ricevuto via SMS al numero di telefono cellulare, dichiarato dal Richiedente in fase di registrazione. Il sistema del Gestore elabora la richiesta, appone la firma FEA (effettuata invocando dei web services esposti dalla Piattaforma di Firma Remota Avanzata del Certificatore Trust Technologies) al *Modulo di Adesione*;
10. L'Incaricato del negozio TIM riceve conferma dal Portale dei Servizi di Identità Digitale del Gestore del completamento della richiesta e del salvataggio nell'area di 'Self-Customer Care' del Richiedente della documentazione prodotta (Modulo di Adesione, Condizioni Generali di Utilizzo e Informativa Privacy);
11. Il Richiedente riceve conferma via e-mail dell'avvenuta emissione delle credenziali e della disponibilità, nella propria area di 'Self-Customer Care' e per tutto il periodo contrattuale, della documentazione sottoscritta digitalmente (Modulo di Adesione, Condizioni Generali di Utilizzo e Informativa Privacy).

Di seguito due diagrammi che rappresentano il flusso sopra descritto:

[4] 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.

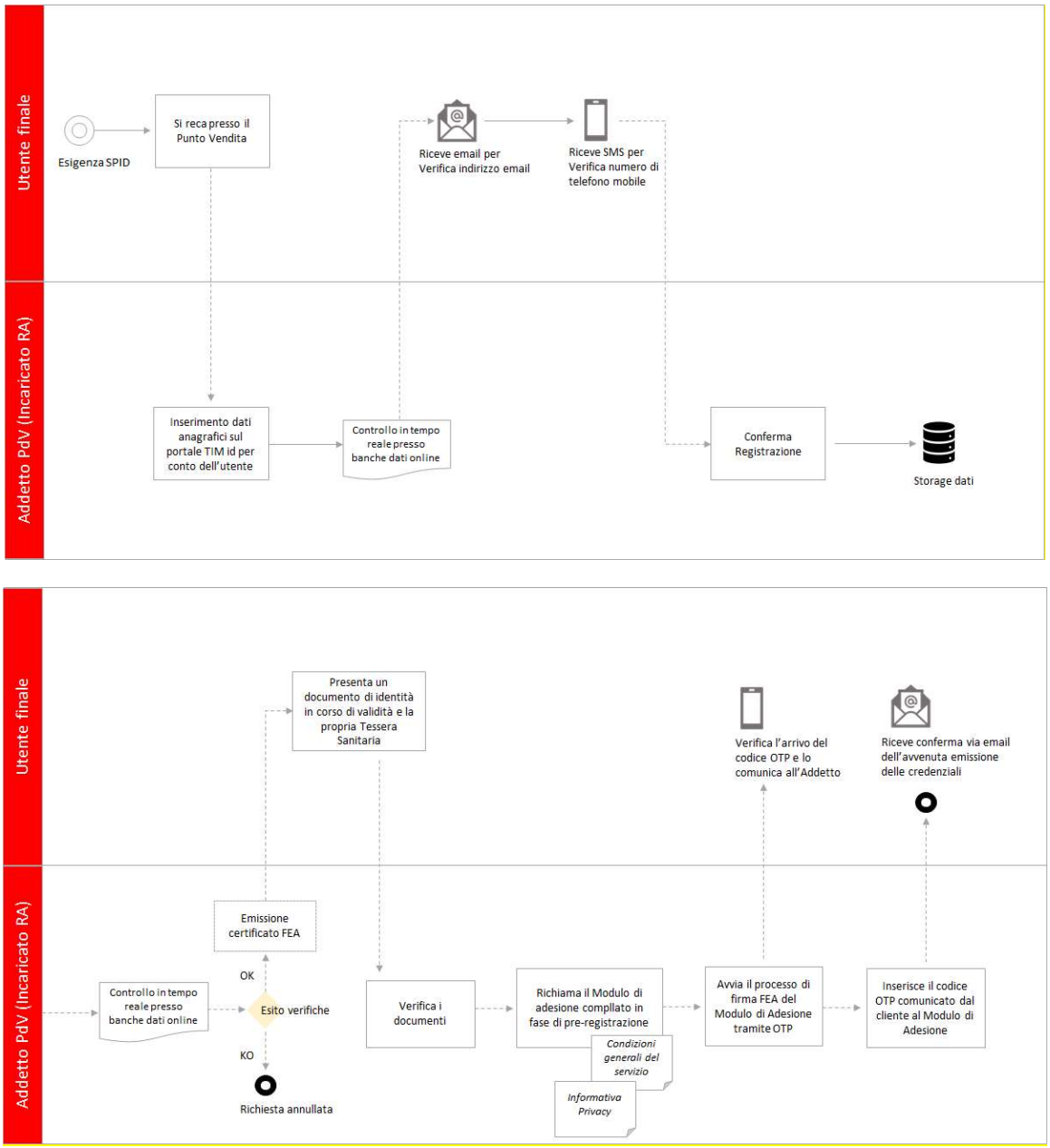

Figura 7 - Flusso di rilascio Identità Digitale per persona fisica con identificazione 'De Visu' presso il negozio TIM

6.2.1.3 Identificazione mediante utilizzo della firma elettronica qualificata o firma digitale

In questa modalità di identificazione il Richiedente opera in autonomia collegandosi via web al servizio online predisposto dal Gestore e viene identificato mediante sottoscrizione di un apposito *Modulo di Adesione* con la propria firma elettronica qualificata[5] (in formato PAdES), per mezzo di strumenti di firma propri.

Questa modalità è composta dai seguenti passi eseguiti in sequenza dal Richiedente e dal Gestore (o Incaricato del Gestore).

[5] A partire dal 01/03/2019, (rif. Avviso SPID n.12 di AgID), i gestori di identità digitale SPID non possono espletare la verifica dell'identità del soggetto richiedente l'identità digitale acquisendo il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale basata su certificati qualificati contenenti l'OID 1.3.76.16.5. Questo OID è presente nei certificati di firma qualificata richiesti tramite identificazione SPID.

6.2.1.3.1 Dimostrazione dell'identità

1. Il Richiedente si collega via web all'apposita sezione del servizio predisposto dal Gestore inserendo il proprio *Codice di Registrazione* ottenuto alla conferma della pre-registrazione e il proprio Codice Fiscale;
2. Il servizio del Gestore mostra a video il *Modulo di Adesione* precompilato con i dati anagrafici validati dal Richiedente in fase di pre-registrazione, contenente anche le Condizioni Generali di Utilizzo del servizio di Identità Digitale e l'Informativa Privacy sul trattamento dei dati personali che devono essere firmati digitalmente dal Richiedente;
3. Il Richiedente effettua il download del *Modulo di Adesione* (formato PDF), lo firma con il proprio strumento di firma ed effettua poi l'upload del file firmato (formato PAdES);
4. Il servizio del Gestore conferma l'avvenuto upload del modulo firmato ed informa il Richiedente in merito all'esito salvo buon fine della procedura di registrazione e alle modalità con le quali gli saranno in seguito consegnate le credenziali relative alla propria Identità Digitale;
5. Il servizio del Gestore verifica il numero di cellulare, dichiarato dal Richiedente in fase di registrazione, mediante invio codice OTP via SMS che viene utilizzato per convalidare i dati identificati; al termine invia una e-mail di conferma contenente i dati riepilogativi.

6.2.1.3.2 Verifica dell'identità (back office)

6. 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 (cfr.3.5);
   b. controlli manuali su fonti autoritative[6] in sostituzione dei controlli automatici(cfr.3.5);
   c. verifica firma digitale[7] 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. ulteriori altre verifiche che si rendessero necessarie.
7. Al termine della verifica dell'identità viene convalida o meno la registrazione:
   a. in caso di esito negativo il sistema del Gestore invia una e-mail al Richiedente con l'esito (KO) della richiesta ed il motivo del rigetto (eventualmente segnalando la necessità di fornire documentazione corretta e/o aggiuntiva presso un PdR),
   b. in caso di esito positivo il sistema del Gestore conferma il completamento della richiesta di adesione e procede all'emissione delle credenziali per il Richiedente;
8. Il sistema del Gestore notifica al Richiedente l'avvenuta emissione delle credenziali con l'invio di una e-mail di conferma contenente i dati riepilogativi e le indicazioni relative alla modalità con la quale gli saranno consegnate;
9. Presso il Gestore viene archiviata la documentazione prodotta nel processo di Registrazione, mediante apposita procedura.

Di seguito un diagramma che rappresenta il flusso sopra descritto:

[6] 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.

[7] 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.

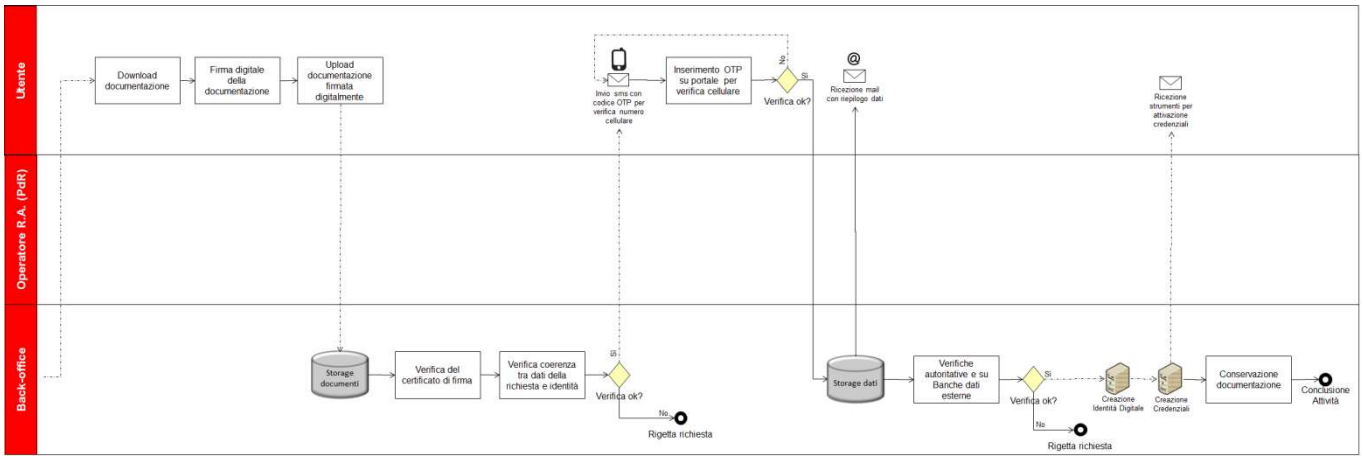

Figura 8 - Flusso di rilascio Identità Digitale per persona fisica con identificazione mediante dispositivo di firma elettronica qualificata o digitale

6.2.1.4 Identificazione mediante utilizzo della carta nazionale dei servizi (CNS) e della carta d'identità elettronica (CIE)

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

Questa modalità è composta dai seguenti passi eseguiti in sequenza dal Richiedente e dal Gestore (o Incaricato del Gestore).

6.2.1.4.1 Dimostrazione dell'identità

1. Il Richiedente si collega via web all'apposita sezione del servizio predisposto dal Gestore inserendo il proprio Codice di Registrazione ottenuto alla conferma della pre-registrazione e il proprio Codice Fiscale;
2. Il servizio del Gestore mostra a video il Modulo di Adesione precompilato con i dati anagrafici validati dal Richiedente in fase di pre-registrazione, contenente anche le Condizioni Generali di Utilizzo del servizio di Identità Digitale e l'Informativa Privacy sul trattamento dei dati personali che devono essere firmati digitalmente dal Richiedente;
3. Il Richiedente conferma gli attributi identificativi, effettua il download del Modulo di Adesione (formato PDF), lo firma per attestazione con la propria carta CNS o CIE ed effettua l'upload del file;
4. Il servizio del Gestore conferma l'avvenuto upload del file ed informa il Richiedente in merito all'esito salvo buon fine della procedura di registrazione e alle modalità con le quali gli saranno in seguito consegnate le credenziali relative alla propria Identità Digitale;
5. Il servizio del Gestore verifica il numero di cellulare, dichiarato dal Richiedente in fase di registrazione, mediante invio codice OTP via SMS che viene utilizzato per convalidare i dati identificati; al termine invia una e-mail di conferma contenente i dati riepilogativi.

6.2.1.4.2 Verifica dell'identità (back office)

6. 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 (cfr.3.5);
   b. controlli manuali su fonti autoritative[8] in sostituzione dei controlli automatici(cfr.3.5);

[8] 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 validità *attestazione* apposta dal Richiedente;

d. verifica corrispondenza e validità dei documenti identificativi indicati dal Richiedente;

e. ulteriori altre verifiche che si rendessero necessarie.

7. Al termine della verifica dell'identità viene convalida o meno la registrazione:

   a. in caso di esito negativo il sistema del Gestore invia una e-mail al Richiedente con l'esito (KO) della richiesta ed il motivo del rigetto (eventualmente segnalando la necessità di fornire documentazione corretta e/o aggiuntiva presso un PdR),

   b. in caso di esito positivo il sistema del Gestore conferma il completamento della richiesta di adesione e procede all'emissione delle credenziali per il Richiedente;

8. Il sistema del Gestore notifica al Richiedente l'avvenuta emissione delle credenziali con l'invio di una e-mail di conferma contenente i dati riepilogativi e le indicazioni relative alla modalità con la quale gli saranno consegnate;

9. Presso il Gestore viene archiviata la documentazione prodotta nel processo di Registrazione, mediante apposita procedura.

Di seguito un diagramma che rappresenta il flusso sopra descritto:

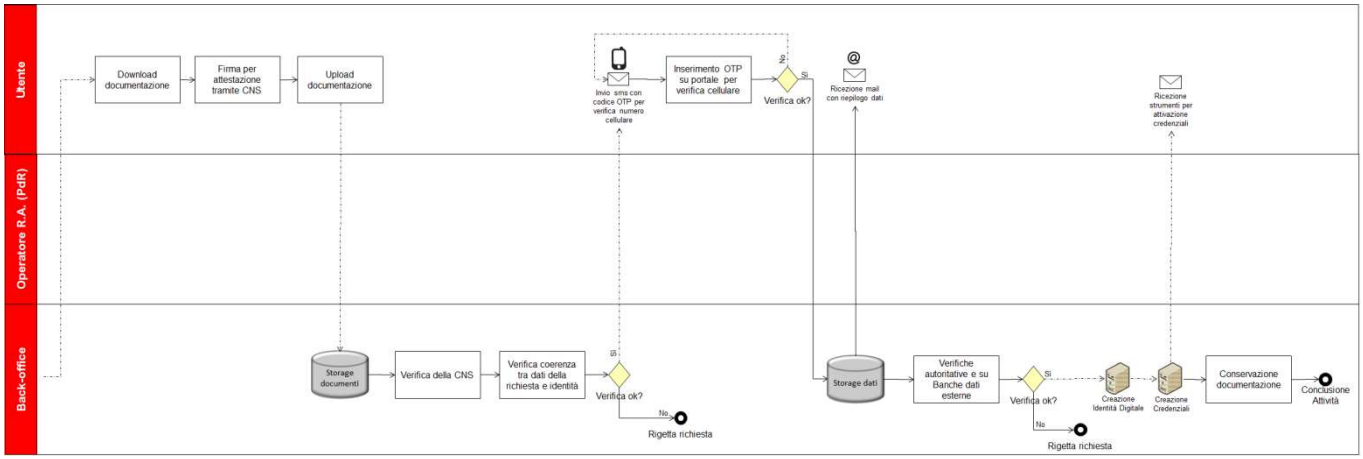

Figura 9 - Flusso di rilascio Identità Digitale per persona fisica con identificazione mediante utilizzo di CNS e CIE

6.2.1.5 Identificazione mediante 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 Registrazione audio-video.

In particolare il Richiedente utilizza il link contenuto nella e-mail ricevuta dal Portale al termine della procedura di pre-registrazione per accedere alla sessione web del *Servizio di Identificazione tramite Registrazione Audio-Video* (SIAV).

Questa modalità è composta dai seguenti passi eseguiti dal Richiedente e dall'Operatore del Gestore (o Incaricato del Gestore).

6.2.1.5.1 Dimostrazione dell'identità

1. Il Richiedente utilizza il link ricevuto dal Portale per accedere alla sessione web del *Servizio di Identificazione tramite Registrazione Audio-Video* (SIAV);
2. L'Operatore del Gestore avvia la sessione web di Identificazione audio-video ed il sistema SIAV crea un *dossier* relativo al Richiedente;
3. 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);

4. Al termine della sessione web il servizio firma digitalmente il *dossier* (contiene *Modulo di Adesione* in formato PDF, foto fronte/retro del documento di identità e della Tessera Sanitaria e il video registrato della sessione di identificazione) che viene automaticamente inviato dal sistema SIAV, unitamente alla registrazione audio-video, in conservazione a norma;

6.2.1.5.2 Verifica dell'identità (remote front office)

5. L'Operatore procede alla verifica delle informazioni acquisite durante la sessione web di identificazione audio-video, mediante:
   a. verifica integrità/qualità della registrazione audio-video;
   b. verifica corrispondenza e validità dei documenti identificativi indicati dal Richiedente;
   c. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni (cfr.3.5);
   d. eventuali controlli manuali su fonti autoritative[9] in sostituzione dei controlli automatici (cfr.3.5);
   e. ulteriori altre verifiche che si rendessero necessarie.
6. Al termine della verifica dell'identità viene convalida o meno la registrazione:
   a. in caso di esito negativo il sistema del Gestore invia una e-mail al Richiedente con l'esito (KO) della richiesta ed il motivo del rigetto (eventualmente segnalando la necessità di fornire documentazione corretta e/o aggiuntiva),
   b. in caso di esito positivo il sistema del Gestore conferma il completamento della richiesta di adesione e procede all'emissione delle credenziali per il Richiedente;
7. Il sistema del Gestore notifica al Richiedente l'avvenuta emissione delle credenziali con l'invio di una e-mail di conferma contenente i dati riepilogativi e le indicazioni relative alla modalità con la quale gli saranno consegnate;
8. Presso il Gestore viene archiviata la documentazione prodotta nel processo di Registrazione, mediante apposita procedura che prevede la possibilità di recupero nel tempo della documentazione posta in conservazione a norma.

Di seguito un diagramma che rappresenta il flusso sopra descritto:

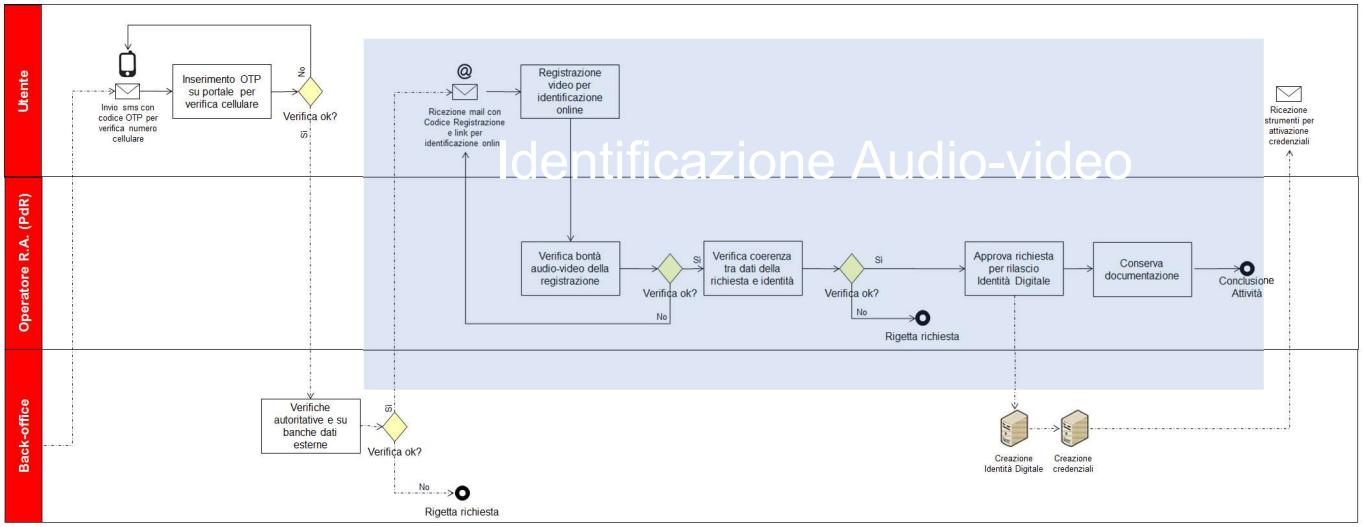

Figura 10 - Flusso di rilascio Identità Digitale per persona fisica con identificazione Audio-Video

[9] 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.

6.2.2 Persona giuridica

6.2.2.1 Identificazione mediante esibizione 'a vista' di un documento di identità ('de visu')

In questa modalità di identificazione il Richiedente si reca presso il Punto di Registrazione (PdR) e viene identificato 'de visu' ossia di persona tramite esibizione a vista di un valido documento d'identità.

Questa modalità è composta dai seguenti passi eseguiti in sequenza prima dal personale di Back-Office presso il Gestore, poi dal Richiedente e dall'Incaricato (dal Gestore) presso il PdR.

6.2.2.1.1 Verifiche documentali (back office) e provisioning certificato di FEA

1. Presso il Gestore il personale di Back-Office procede alle verifiche documentali ovvero delle informazioni presenti nella Scheda di Registrazione mediante:
   a. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni (cfr.3.5),
   b. eventuali controlli manuali su fonti autoritative[10] in sostituzione dei controlli automatici (cfr.3.5),
   c. verifica validità[11] della documentazione di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del Richiedente l'identità digitale per conto della persona giuridica,
   d. effettuata l'associazione <Amministratore o Rappresentante legale – Persona giuridica>, procede alla identificazione 'de visu' - come persona fisica - dell'Amministratore o del legale rappresentante (come indicato al paragrafo §6.2.1.1);
2. Al termine delle verifiche il Back-Office convalida la richiesta ed il sistema del Gestore avvia il provisioning del Certificato di FEA associato al Richiedente (effettuato invocando dei web services esposti dalla Piattaforma di Firma Remota Qualificata del Certificatore Trust Technologies). Il Certificato di FEA è emesso da una Certification Authority non accreditata e verrà utilizzato per firmare la documentazione contrattuale del Richiedente con il Gestore;

6.2.2.1.2 Dimostrazione dell'identità

3. Presso il PdR il Richiedente presenta il proprio *Codice di Registrazione* ottenuto alla conferma della pre-registrazione;
4. L'Incaricato presso il PdR accede al Portale dei Servizi di Identità Digitale con le proprie credenziali, inserisce il *Codice di Registrazione* presentato dal Richiedente e richiama a video la Scheda di Registrazione con i relativi dati anagrafici;
5. Il Richiedente presenta un documento di identità in corso di validità e la propria Tessera Sanitaria (come evidenza del Codice Fiscale);

6.2.2.1.3 Verifica dell'identità (front office)

6. L'Incaricato presso il PdR procede alla verifica dell'identità ovvero verifica la corrispondenza tra documenti identificativi presentati e presenza fisica del richiedente ('de-visu');
7. L'Incaricato presso il PdR richiama a video il *Modulo di Adesione* precompilato con i dati anagrafici validati dal Richiedente in fase di pre-registrazione, contenente anche le Condizioni Generali di Utilizzo del servizio di Identità Digitale e l'Informativa Privacy sul trattamento dei dati personali che vengono confermate dal Richiedente tramite apposizione firma FEA. L'Incaricato presso il PdR avvia la verifica del numero di

[10] 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.

[11] 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.

cellulare, dichiarato dal Richiedente in fase di registrazione, ed avvia il processo di firma FEA del *Modulo di Adesione* tramite OTP;

8. Il Richiedente comunica all'Incaricato presso il PdR il codice OTP ricevuto via SMS che viene utilizzato per convalidare i dati identificati e per firmare digitalmente il *Modulo di Adesione*;
9. L'Incaricato presso il PdR inserisce il codice OTP sul Portale dei Servizi di Identità Digitale. Il codice OTP inserito è quello che il Richiedente ha ricevuto via SMS al numero di telefono cellulare, dichiarato in fase di registrazione. Il sistema del Gestore elabora la richiesta, appone la firma FEA (effettuata invocando dei web services esposti dalla Piattaforma di Firma Remota Qualificata del Certificatore Trust Technologies) al *Modulo di Adesione*;
10. L'Incaricato presso il PdR riceve conferma dal Portale dei Servizi di Identità Digitale del Gestore del completamento della richiesta e del salvataggio nell'area di 'Self-Customer Care' del Richiedente della documentazione prodotta (Modulo di Adesione, Condizioni Generali di Utilizzo e Informativa Privacy);
11. Il Richiedente riceve conferma via e-mail dell'avvenuta emissione delle credenziali e della disponibilità, nella propria area di 'Self-Customer Care' e per tutto il periodo contrattuale, della documentazione sottoscritta digitalmente (Modulo di Adesione, Condizioni Generali di Utilizzo e Informativa Privacy).

Di seguito un diagramma che rappresenta il flusso sopra descritto:

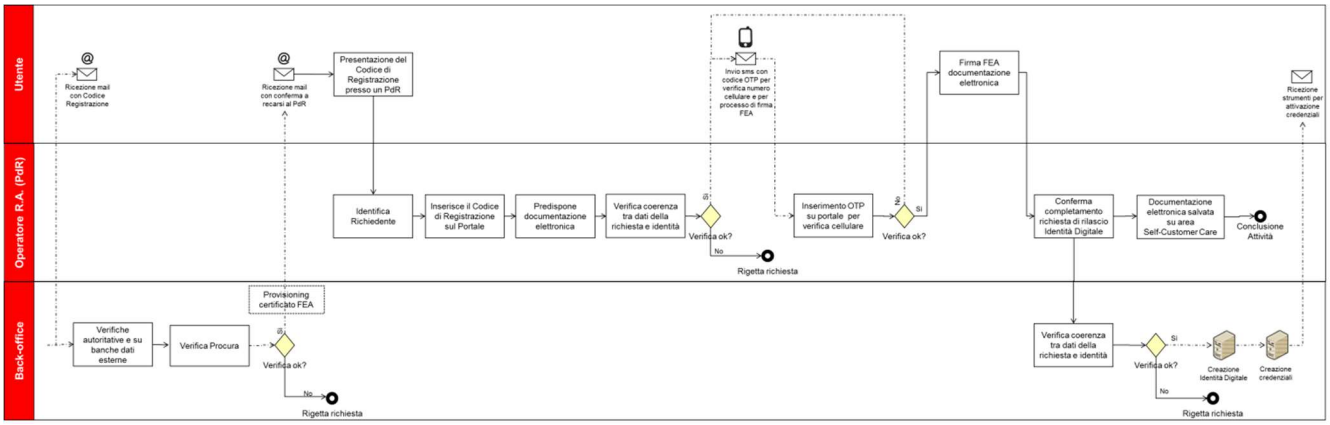

Figura 11 - Flusso di rilascio Identità Digitale per persona giuridica con identificazione 'De Visu'

6.2.2.2 Identificazione mediante utilizzo della firma elettronica qualificata o firma digitale

In questa modalità di identificazione il Richiedente opera in autonomia collegandosi via web al servizio online predisposto dal Gestore e viene identificato mediante sottoscrizione di un apposito *Modulo di Adesione* con la propria firma elettronica qualificata (in formato PAdES), per mezzo di strumenti di firma propri.

Questa modalità è composta dai seguenti passi eseguiti in sequenza dal Richiedente e dal Gestore (o Incaricato del Gestore).

6.2.2.2.1 Dimostrazione dell'identità

1. Il Richiedente si collega via web all'apposita sezione del servizio predisposto dal Gestore inserendo il proprio *Codice di Registrazione* ottenuto alla conferma della pre-registrazione e il proprio Codice Fiscale;
2. Il servizio del Gestore mostra a video il *Modulo di Adesione* precompilato con i dati anagrafici validati dal Richiedente in fase di pre-registrazione, contenente anche le Condizioni Generali di Utilizzo del servizio di Identità Digitale e l'Informativa Privacy sul trattamento dei dati personali che devono essere firmati digitalmente dal Richiedente;
3. Il Richiedente effettua il download del *Modulo di Adesione* (formato PDF), lo firma con il proprio strumento di firma ed effettua poi l'upload del file firmato (formato PAdES);
4. Il Richiedente effettua inoltre l'upload del documento di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del richiedente l'identità digitale per conto della persona giuridica: *Visura Camerale*

firmata digitalmente dalla CCIAA o, in alternativa, *Copia dell'Atto notarile di Procura legale* firmata digitalmente dal Richiedente;

5. Il servizio del Gestore conferma l'avvenuto upload dei file firmati ed informa il Richiedente in merito all'esito salvo buon fine della procedura di registrazione e alle modalità con le quali gli saranno in seguito consegnate le credenziali relative alla propria Identità Digitale;
6. Il servizio del Gestore verifica il numero di cellulare, dichiarato dal Richiedente in fase di registrazione, mediante invio codice OTP via SMS che viene utilizzato per convalidare i dati identificati; al termine invia una e-mail di conferma contenente i dati riepilogativi.

6.2.2.2.2 Verifica dell'identità (back office)

7. 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 (cfr.3.5);
    b. controlli manuali su fonti autoritative[12] in sostituzione dei controlli automatici (cfr.3.5);
    c. verifica validità[13] della documentazione di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del Richiedente l'identità digitale per conto della persona giuridica;
    d. effettuata l'associazione <Amministratore o Rappresentante legale – Persona giuridica>, si procede alla identificazione mediante firma elettronica qualifica o digitale - come persona fisica - dell'Amministratore o del legale rappresentante (come indicato al paragrafo §6.2.1.2).
    e. ulteriori altre verifiche che si rendessero necessarie.
8. Al termine della verifica dell'identità viene convalida o meno la registrazione:
    a. in caso di esito negativo il sistema del Gestore invia una e-mail al Richiedente con l'esito (KO) della richiesta ed il motivo del rigetto (eventualmente segnalando la necessità di fornire documentazione corretta e/o aggiuntiva presso un PdR),
    b. in caso di esito positivo il sistema del Gestore conferma il completamento della richiesta di adesione e procede all'emissione delle credenziali per il Richiedente;
9. Il sistema del Gestore notifica al Richiedente l'avvenuta emissione delle credenziali con l'invio di una e-mail di conferma contenente i dati riepilogativi e le indicazioni relative alla modalità con la quale gli saranno consegnate;
10. Presso il Gestore viene archiviata la documentazione prodotta nel processo di Registrazione, mediante apposita procedura.

Di seguito un diagramma che rappresenta il flusso sopra descritto:

[12] 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.

[13] 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.

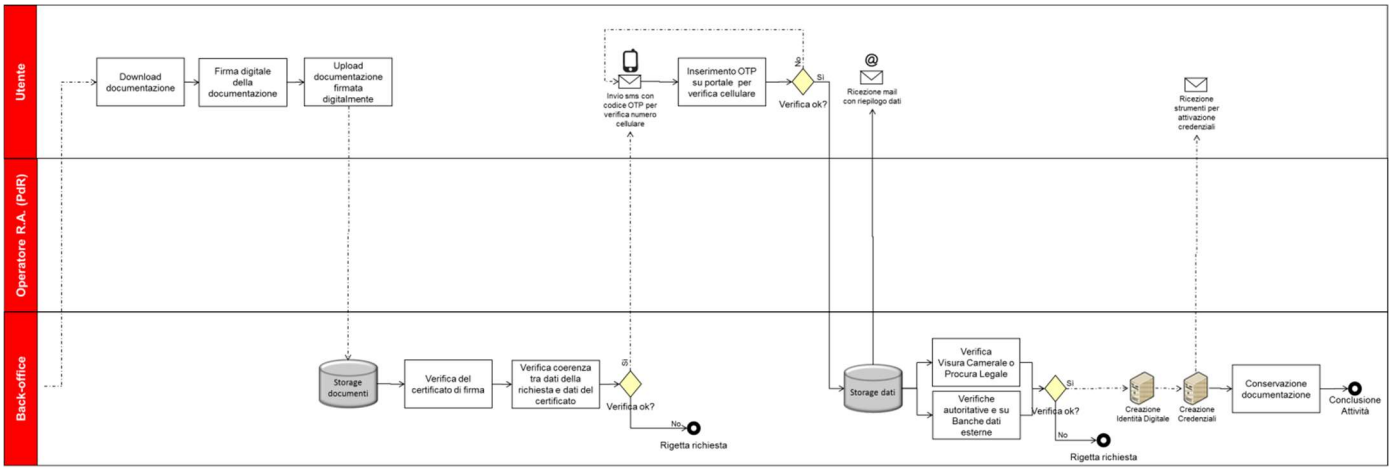

Figura 35 - Flusso di rilascio Identità Digitale per persona giuridica con identificazione mediante dispositivo di firma elettronica qualificata o digitale

6.2.2.3 Identificazione 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 e 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.

Questa modalità è composta dai seguenti passi eseguiti in sequenza dal Richiedente e dal Gestore (o Incaricato del Gestore).

6.2.2.3.1 Dimostrazione dell'identità

1. Il Richiedente si collega via web all'apposita sezione del servizio predisposto dal Gestore inserendo il proprio Codice di Registrazione ottenuto alla conferma della pre-registrazione e il proprio Codice Fiscale;
2. Il servizio del Gestore mostra a video il Modulo di Adesione precompilato con i dati anagrafici validati dal Richiedente in fase di pre-registrazione, contenente anche le Condizioni Generali di Utilizzo del servizio di Identità Digitale e l'Informativa Privacy sul trattamento dei dati personali che devono essere firmati digitalmente dal Richiedente;
3. Il Richiedente conferma gli attributi identificativi, effettua il download del Modulo di Adesione (formato PDF), lo firma per attestazione con la propria carta CNS ed effettua l'upload del file;
4. Il Richiedente effettua inoltre l'upload del documento di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del richiedente l'identità digitale per conto della persona giuridica: *Visura Camerale* firmata digitalmente dalla CCIAA o, in alternativa, *Copia dell'Atto notarile di Procura legale* firmata digitalmente dal Richiedente;
5. Il servizio del Gestore conferma l'avvenuto upload dei file firmati ed informa il Richiedente in merito all'esito salvo buon fine della procedura di registrazione e alle modalità con le quali gli saranno in seguito consegnate le credenziali relative alla propria Identità Digitale;
6. Il servizio del Gestore verifica il numero di cellulare, dichiarato dal Richiedente in fase di registrazione, mediante invio codice OTP via SMS che viene utilizzato per convalidare i dati identificati; al termine invia una e-mail di conferma contenente i dati riepilogativi.

6.2.2.3.2 Verifica dell'identità (back office)

7. 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 (cfr.3.5);

b. controlli manuali su fonti autoritative[14] in sostituzione dei controlli automatici (cfr.3.5);

c. verifica validità[15] della documentazione di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del Richiedente l'identità digitale per conto della persona giuridica;

d. effettuata l'associazione <Amministratore o Rappresentante legale – Persona giuridica>, si procede alla identificazione mediante carta CNS o CIE - come persona fisica - dell'Amministratore o del legale rappresentante (come indicato al paragrafo §6.2.1.4);

e. ulteriori altre verifiche che si rendessero necessarie.

8. Al termine della verifica dell'identità viene convalida o meno la registrazione:

   a. in caso di esito negativo il sistema del Gestore invia una e-mail al Richiedente con l'esito (KO) della richiesta ed il motivo del rigetto (eventualmente segnalando la necessità di fornire documentazione corretta e/o aggiuntiva presso un PdR),

   b. in caso di esito positivo il sistema del Gestore conferma il completamento della richiesta di adesione e procede all'emissione delle credenziali per il Richiedente;

9. Il sistema del Gestore notifica al Richiedente l'avvenuta emissione delle credenziali con l'invio di una e-mail di conferma contenente i dati riepilogativi e le indicazioni relative alla modalità con la quale gli saranno consegnate;

10. Presso il Gestore viene archiviata la documentazione prodotta nel processo di Registrazione, mediante apposita procedura.

Di seguito un diagramma che rappresenta il flusso sopra descritto:

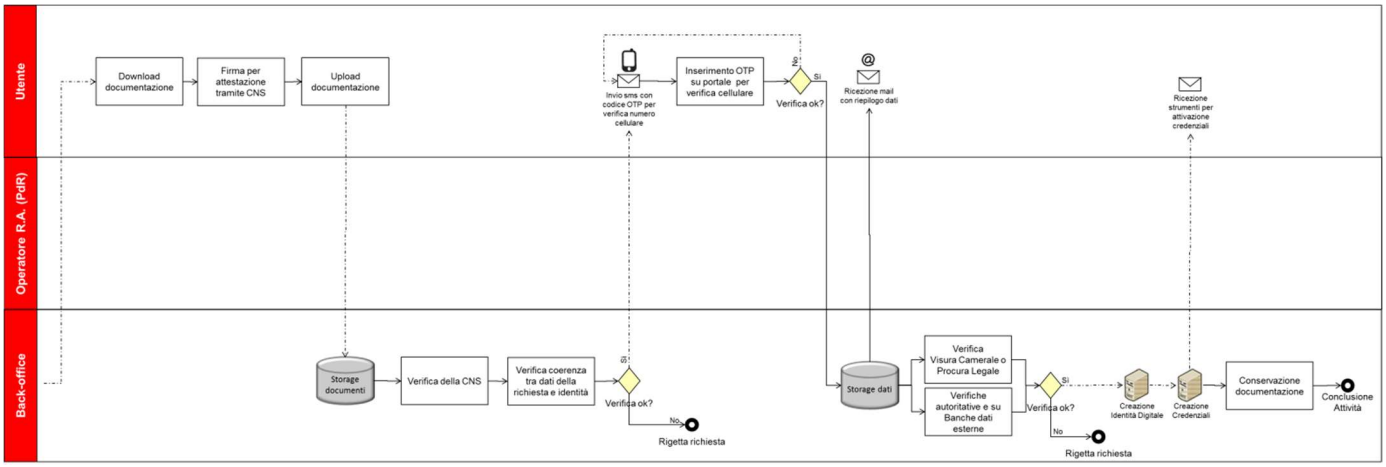

Figura 46 - Flusso di rilascio Identità Digitale per persona giuridica con identificazione mediante utilizzo di CNS o CIE

[14] 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.

[15] 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.

6.2.2.4 Identificazione mediante 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 Registrazione audio-video.

In particolare, il Richiedente utilizza il link contenuto nella e-mail ricevuta dal Portale al termine della procedura di pre-registrazione per accedere alla sessione web del *Servizio di Identificazione tramite Registrazione Audio-Video* (SIAV).

Questa modalità è composta dai seguenti passi eseguiti in sequenza dal Richiedente e dall'Operatore del Gestore (o Incaricato del Gestore).

6.2.2.4.1 Dimostrazione dell'identità

1. Il Richiedente utilizza il link ricevuto dal Portale per accedere alla sessione web del Servizio di Identificazione tramite Registrazione Audio-Video (SIAV);
2. L'Operatore del Gestore avvia la sessione web di Identificazione audio-video ed il sistema SIAV crea un *dossier* relativo al Richiedente;
3. 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 giuridiche;
4. Il Richiedente dichiara che si presenta in qualità di Amministratore o Rappresentante Legale per conto di una Persona Giuridica, dichiarandone esplicitamente Ragione Sociale, Partita IVA e Sede Legale;
5. L'Operatore prende atto di quanto dichiarato (che viene registrato nel file audio-video) e procede con l'identificazione del Richiedente quale persona fisica, avvia la registrazione della sessione web Audio-Video interagendo con il Richiedente in base alla specifica procedura dedicata all'identificazione delle persone fisiche, che prevede anche l'acquisizione da webcam delle foto del documento di identità e del codice fiscale;
6. Al termine della sessione web l'Operatore firma digitalmente il *dossier* (contiene *Modulo di Adesione* in formato PDF, foto fronte/retro del documento di identità e del codice fiscale) che viene automaticamente inviato dal sistema SIAV, unitamente alla registrazione audio-video, in conservazione a norma;

6.2.2.4.2 Verifica dell'identità (remote front office)

7. L'Operatore procede alla verifica delle informazioni acquisite durante la sessione web di identificazione audio-video, mediante:
   a. verifica integrità/qualità della registrazione audio-video;
   b. verifica corrispondenza e validità dei documenti identificativi indicati dal Richiedente;
   c. verifica corrispondenza e validità dei dati dichiarati dal Richiedente in qualità di Amministratore o Rappresentante Legale per conto della Persona Giuridica;
   d. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni (cfr.3.5);
   e. eventuali controlli manuali su fonti autoritative[16] in sostituzione dei controlli automatici (cfr.3.5);
   f. ulteriori altre verifiche che si rendessero necessarie.
8. Al termine della verifica dell'identità viene convalida o meno la registrazione:
   a. in caso di esito negativo il sistema del Gestore invia una e-mail al Richiedente con l'esito (KO) della richiesta ed il motivo del rigetto (eventualmente segnalando la necessità di fornire documentazione corretta e/o aggiuntiva),
   b. in caso di esito positivo il sistema del Gestore conferma il completamento della richiesta di adesione e procede all'emissione delle credenziali per il Richiedente;
9. Il sistema del Gestore notifica al Richiedente l'avvenuta emissione delle credenziali con l'invio di una e-mail di conferma contenente i dati riepilogativi e le indicazioni relative alla modalità con la quale gli saranno consegnate;
10. Presso il Gestore viene archiviata la documentazione prodotta nel processo di Registrazione, mediante apposita procedura che prevede la possibilità di recupero nel tempo della documentazione posta in conservazione a norma.

[16] 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.

Di seguito un diagramma che rappresenta il flusso sopra descritto:

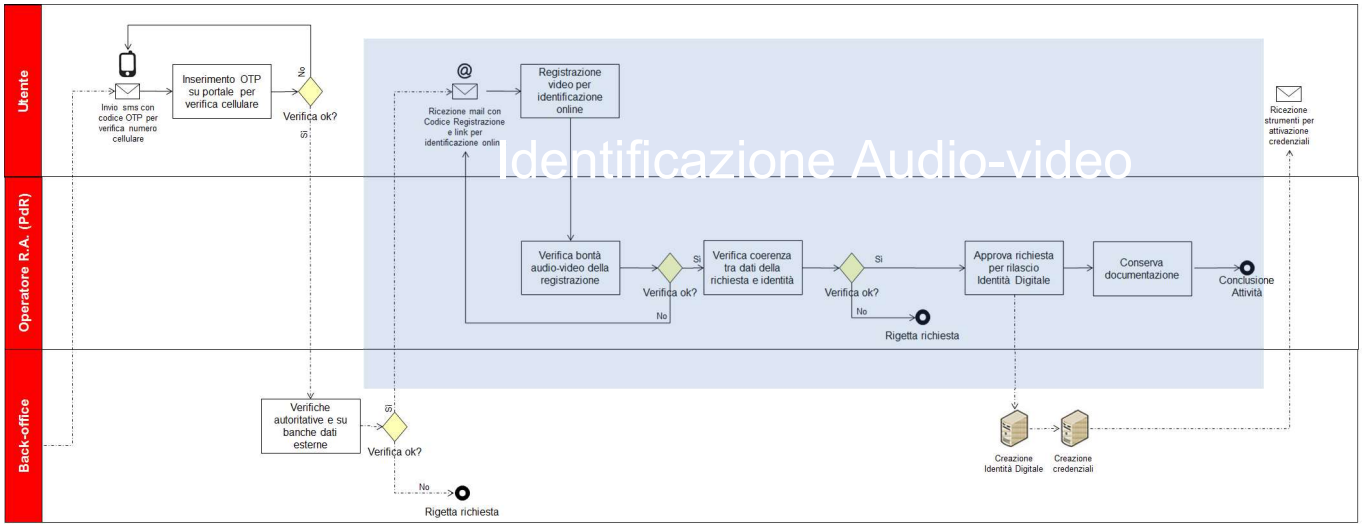

Figura 57 - Flusso di rilascio Identità Digitale per persona giuridica con identificazione Audio-Video

6.3 Creazione 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.

L'identità in questa fase risulterà in uno stato non attivo poiché non è stata ancora resa operativa da parte dell'utente finale con il processo di *consegna delle credenziali e delle informazioni per l'utilizzo del servizio*.

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

7 Gestione delle credenziali

La fase di **gestione delle credenziali** comprende tutti i processi relativi alla gestione del ciclo di vita di una credenziale. Alcuni di questi processi dipendono dal fatto se le credenziali sono trasportate o meno su un dispositivo hardware.

Il processo di ***emissione*** delle credenziali è il processo di fornire o in altri termini di 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 (che sono in uno stato non attivo per motivi di sicurezza).

Il processo di ***consegna*** rappresenta l'ultima fase relativamente al processo di rilascio di una identità digitale: la complessità varia con il livello di Assurance (LoA) necessario.

7.1 Credenziali di Livello 1 SPID (LoA2)

7.1.1 [*LoA2 Password*]

7.1.1.1 Descrizione

Password alfanumerica (un fattore) secondo il livello LoA2 dello standard ISO/IEC DIS 29115.

7.1.1.2 Consegna

Per la consegna delle credenziali di Livello 1 la modalità è la seguente:

- la piattaforma di gestione del servizio invia all'utente
  - *UserID* via e-mail, utilizzando l'indirizzo e-mail dichiarato e verificato in fase di Registrazione;
  - *Codice di Attivazione della Password* (valido solo per il primo accesso, consente all'Utente di definire la propria Password) via SMS, utilizzando il numero di telefono cellulare dichiarato e verificato in fase di Registrazione;
- al primo accesso dell'utente la piattaforma chiederà l'inserimento del Codice di Attivazione ricevuto per SMS, dopodiché l'utente dovrà definire una propria *Password* per il servizio (secondo la password policy di sicurezza impostata sulla piattaforma);
- la piattaforma di gestione del servizio confermerà l'attivazione della credenziale per l'utente.

7.2 Credenziali di Livello 2 SPID (LoA3)

7.2.1 [*(LoA2 Password) + (One-Time Password via SMS)*]

7.2.1.1 Descrizione

Password abbinata a un Codice OTP inviato via SMS (due fattori) secondo il livello LoA3 dello standard ISO/IEC DIS 29115.

Il secondo fattore è realizzato mediante un *Token out-of-band* indirizzabile in modo univoco che può ricevere un codice/segreto per essere usato una sola volta durante la sessione di servizio (invio di SMS al numero di telefono cellulare dichiarato dal titolare e verificato in sede di registrazione).

7.2.1.2 Consegna

Per la consegna delle credenziali di Livello 2 non è necessario altro oltre quanto previsto per la consegna delle credenziali di Livello1, il numero di telefono cellulare è già verificato.

8 Autenticazione

Il processo di **autenticazione** prevede l'uso di un determinato protocollo per dimostrare il possesso e/o il controllo di una credenziale per stabilire la fiducia in una identità.

I requisiti del protocollo di autenticazione variano a seconda del livello di garanzia (*Livello di Assurance* o *LoA*) applicabile. Nello SPID l'autenticazione a più fattori è richiesta ai livelli di garanzia 2 (LoA3) e 3 (LoA4).

8.1 Gestione delle richieste di autenticazione

La gestione delle richieste di autenticazione provenienti da un Service Provider, avviene per il Gestore attraverso la verifica delle credenziali presentate dall'utente e il rilascio di un'asserzione di autenticazione SAML v2.0 contenente gli attributi associati all'identità digitale corrispondente.

La piattaforma di servizio del Gestore implemena il profilo SAML "Web Browser SSO *SP-Initiated",* nelle due versioni previste dalla normativa: *"Redirect -> POST binding*" e "*POST -> POST binding*". In questo profilo il meccanismo di autenticazione è innescato dalla richiesta di accesso a un servizio effettuata dall'utente (tramite il suo browser web) ad un fornitore di servizi (il Service Provider). Il Service Provider a sua volta si rivolge all'Identity Provider (il Gestore) in modalità "pull". La piattaforma permette di ricevere le richieste di autenticazione SAML (basata sul costrutto <AuthnRequest>) usando il binding HTTP-Redirect o il binding HTTP-POST.

La relativa risposta SAML (basata sul costrutto <Response>) è inviata al Service Provider tramite il binding HTTP-POST.

Il Gestore supporta tutti i formati ammessi dallo standard SAMLv2.0 in merito alle asserzioni, alle richieste di <AuthnRequest> con relative risposte <Response> e del binding.

8.2 Meccanismi di autenticazione

Il processo di verifica delle credenziali utente (l'**autenticazione**), implementato dalla piattaforma del Gestore TI Trust Technologies per il rilascio di un'asserzione, è in grado di assicurare i seguenti livelli di sicurezza:

- **Livello di sicurezza 1 (LoA2 dello standard ISO/IEC 29115)** – sistemi di autenticazione informatica ad un fattore (password o parola chiave);
- **Livello di sicurezza 2 (LoA3 dello standard ISO/IEC 29115)** – sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo;

8.2.1 Meccanismi di autenticazione informatica a Livello 1 SPID (LoA2)

8.2.1.1 [*LoA2 Password*]

Per il Livello di sicurezza 1 SPID (LoA2 dello standard ISO/IEC 29115) la piattaforma del Gestore offre l'autenticazione ad un fattore tramite **una Password.**

L'autenticazione informatica a Livello 1 (LoA2) che il Gestore mette a disposizione è realizzata pertanto mediante:

- inserimento di *UserID & Password*.

Il livello di sicurezza assicurato dall'autenticazione ad un fattore si basa sulla complessità della password, la cui policy di definizione e gestione è in linea con le best practices di riferimento e conforme a quanto stabilito dall'AgID nelle modalità attuative SPID.

Il servizio prevede il blocco temporaneo delle credenziali dopo un numero, configurabile, di tentativi di autenticazione falliti (es. per inserimento di una password errata).

8.2.2 Meccanismi di autenticazione informatica a Livello 2 SPID (LoA3)

8.2.2.1 [*(LoA2 Password) + (One-Time Password via SMS)*]

Per il Livello di sicurezza 2 SPID (LoA3 dello standard ISO/IEC 29115), la piattaforma offre l'autenticazione a due fattori tramite **una Password e un codice OTP inviato via SMS**.

L'autenticazione informatica a Livello 2 (LoA3) che il Gestore mette a disposizione è realizzata mediante una combinazione multi-token, in dettaglio:

- inserimento di *UserID &* Password (quelle del Livello 1 SPID), e
- inserimento del ***codice OTP*** ricevuto via SMS dal titolare.

Il secondo fattore è realizzato mediante invio di codice OTP via SMS al numero di telefono cellulare dichiarato dal titolare e verificato in sede di registrazione, tale codice temporaneo ha una validità limitata nel tempo, configurabile.

Il servizio prevede il blocco delle credenziali dopo un numero, configurabile, di tentativi di autenticazione falliti (es. inserimento codice OTP o della password errati).

Il secondo fattore è rappresentato dal telefono cellulare e l'autenticazione è rafforzata attraverso la dimostrazione della disponibilità dell'apparato al momento dell'operazione con utilizzo del numero telefonico cellulare dichiarato dal titolare e verificato in fase di registrazione dal Gestore.

9 Registro delle attività

Questo registro deve contenere le informazioni e la documentazione della fase di registrazione che è stata raccolta (e può essere conservata), le informazioni sul processo di verifica delle informazioni di identità, i risultati di questi passaggi, e altri dati pertinenti.

Il Gestore conserva i dati utilizzati per la verifica dell'identità di una persona fisica, in particolare:

- per l'identificazione effettuata 'de visu', gli estremi e la copia per immagine del documento di identità e della tessera sanitaria;
- per l'identificazione effettuata con Firma Elettronica Qualificata, il Modulo di Richiesta firmato digitalmente;
- per l'identificazione effettuata con carta CNS, l'attestazione del Modulo di Richiesta;
- per l'identificazione effettuata con Sistemi di Registrazione Audio-Video, il *dossier* creato dal sistema che contiene le copie per immagine del documento di identità e della tessera sanitaria e il file audio-video della registrazione.

Il Gestore conserva i dati utilizzati per la verifica dell'identità di una persona giuridica, in particolare:

- per l'identificazione effettuata 'de visu', gli estremi e la copia per immagine del documento di identità e della tessera sanitaria dell'Amministratore o Rappresentante legale e la Certificazione attestante lo stato di Amministratore o Rappresentante legale del soggetto Richiedente l'identità per conto della persona giuridica;
- per l'identificazione effettuata con Firma Elettronica Qualificata, il Modulo di Richiesta firmato digitalmente e la Certificazione attestante lo stato di Amministratore o Rappresentante legale del soggetto Richiedente l'identità per conto della persona giuridica firmata digitalmente;
- per l'identificazione effettuata con carta CNS o CIE, l'attestazione del Modulo di Richiesta e la Certificazione attestante lo stato di Amministratore o Rappresentante legale del soggetto Richiedente l'identità per conto della persona giuridica firmata digitalmente;
- per l'identificazione effettuata con Sistemi di Registrazione Audio-Video, il *dossier* creato dal sistema che contiene le copie per immagine del documento di identità e della tessera sanitaria e il file audio-video della registrazione.

Appropriate registrazioni vengono conservate per tutto il ciclo di vita di una credenziale. Come minimo, i registri sono mantenuti per documentare le seguenti informazioni:

a) La creazione di una credenziale,

b) L'identificativo della credenziale,

c) Il soggetto (persona fisica o giuridica) al quale è stata rilasciata la credenziale, e

d) Lo stato della credenziale.

Le registrazioni devono essere mantenute per ogni processo coinvolto nella fase di gestione delle credenziali. Se le credenziali vengono rilasciate ai soggetti persone fisiche, la tenuta di registri può comportare il trattamento di informazioni di identificazione personale.

9.1 Conservazione dei documenti (per la registrazione delle identità)

È il processo di archiviazione e conservazione sicura delle informazioni collezionate dal *Registro delle attività* durante la fase di *Registrazione e verifica dell'identità*.

Il *Registro delle attività* è il processo di archiviazione e conservazione sicura della documentazione relativa alla fase di registrazione in cui viene creato un apposito fascicolo elettronico. Questo registro deve contenere le informazioni e la documentazione che sono state raccolte (e possono essere conservate), le informazioni sul processo di verifica delle informazioni di identità, i risultati di questi passaggi, e altri dati pertinenti.

È prevista l'implementazione di un registro informatico che deve contenere, in un apposito fascicolo elettronico, le informazioni e la documentazione raccolta, le informazioni sul processo di verifica delle informazioni di identità, i risultati di questi passaggi, e gli altri dati pertinenti.

Il Gestore conserva i dati utilizzati per la verifica dell'identità personale di ciascun utente, in particolare:

- gli estremi e la copia per immagine del documento di identità e della tessera sanitaria,
- il modulo di richiesta,
- la Certificazione attestante lo stato di Amministratore o Rappresentante legale del soggetto Richiedente l'identità per conto della persona giuridica,
- il *dossier* creato dal sistema che contiene le copie per immagine del documento di identità e della tessera sanitaria e il file audio-video della registrazione.

Tutta la documentazione inerente al processo di registrazione viene conservata e trattata come indicato dall'art. 7 commi 8 e 9 del DPCM SPID. Il Gestore del servizio dovrà quindi conservarli per tutta la durata contrattuale e trasmetterli alla scadenza del contratto all'Agenzia per l'Italia Digitale o a soggetto da questa indicato.

9.2 Tracciatura delle operazioni di verifica dell'identità e modalità di acquisizione

Il sistema traccia in un apposito repository (Fascicolo dell'Utente – cartella su disco) tutte le operazioni di verifica effettuate dal sistema.

Esistono diversi tipi di verifica:

- le verifiche manuali, effettuate da un operatore della Registration Authority (RA) o del Back-Office;
- le verifiche automatiche effettuate verso sistemi/servizi esterni (ad esempio servizio SCIPAFI);
- le verifiche relative alla Firma Qualificata (FQ) e alla Carta Nazionale dei Servizi (CNS) e alla Carta di Identità Elettronica (CIE).

In particolare l'operatore della Registration Authority è colui che identifica il cittadino al fine del rilascio dell'identità digitale.

Le evidenze prodotte dai diversi tipi di verifica sono in generale dei file che contengono dettagli sulla verifica effettuata e sul relativo esito:

- Richiesta / Risposta, nel caso di verifiche effettuate invocando un sistema / servizio esterno (ad esempio interrogazioni del sistema SCIPAFI);
- File caricati a sistema e relative note, nel caso di verifiche manuali effettuate da un operatore (ad esempio l'identificazione di un cittadino da parte dell'operatore della Registration Authority);
- Richiesta / Risposta, tracciamento del dettaglio dell'esito, CRL contattata, eventuali errori nel caso delle verifiche relative alla Firma Qualificata, alla CNS o alla CIE.

Gli operatori che utilizzano il sistema sono a loro volta identificati dal processo di autenticazione e il loro identificativo (ID operatore) viene tracciato in tutte le evidenze (file) salvate nel Fascicolo dell'Utente.

In questa maniera a ciascuna evidenza relativa ad una determinata operazione effettuata sul sistema (identificazione di un cittadino, verifica dei dati su un sistema esterno, ecc.) viene associato l'identificativo dell'operatore che ha effettuato l'operazione/verifica.

Nel caso di verifiche automatiche effettuate in autonomia (ovvero senza l'intervento diretto di un operatore) dal sistema, viene tracciato l'ID di un utente di sistema, utilizzato per le operazioni automatiche. In questo modo è possibile, in caso di controlli, disambiguare se una operazione è stata effettuata da un operatore o in automatico dal sistema.

Per garantire l'integrità delle evidenze delle verifiche i file con gli esiti salvati nel Fascicolo dell'Utente vengono firmati con un sistema di marca temporale che genera la marca e la firma per tutti i file contenenti gli esiti e ne impedisce la modifica.

9.3 Conservazione dei documenti previsti dalla normativa per la modifica dell'identità digitale

Tutta la documentazione fornita durante le attività di modifica dell'Identità Digitale (Moduli di richiesta di sospensione o di revoca, documenti di riconoscimento allegati, denunce di smarrimento, notifica dell'avvenuta variazione dello stato dell'Identità Digitale) deve essere conservata dal Gestore per la durata contrattuale e trasmetterli alla scadenza del contratto all'Agenzia per l'Italia Digitale o a soggetto da questa indicato.

È inoltre prevista la possibilità di archiviare tutta la documentazione sopra indicata tramite il servizio di Conservazione a Norma.

9.4 Tracciatura degli accessi al servizio di autenticazione e modalità di acquisizione

Nella fase di autenticazione possono essere necessari monitoraggio e registrazione degli eventi per una varietà di scopi, come fornitura di servizi, conformità, responsabilità, e/o requisiti di legge.

Il tracciamento di ogni evento di utilizzo delle credenziali di accesso attraverso le funzionalità native di log e auditing per un monitoraggio continuo dell'utilizzo del servizio al fine rilevare usi impropri (a titolo esemplificativo e non esaustivo, *brute force attack*, accessi a indirizzi IP differenti o *denial of service*) o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, permettono di attivare delle azioni preventive di sospensione dell'identità digitale in caso di attività sospetta.

Dove sono interessati utenti persone fisiche, le informazioni contenute in tali registri possono contenere informazioni sensibili. Tali registrazioni devono essere gestite in modo da tenere conto della necessità di proteggere e ridurre al minimo informazioni di identificazione personale.

Durante le normali attività di accesso ai servizi, tutti gli utenti verranno sottoposti ad autenticazione e autorizzazione effettuata dalle componenti di *Siteminder* e *AuthMinder*. Tutte queste operazioni, ovviamente, genereranno una serie di eventi associati ad uno specifico esito, positivo o negativo, che guideranno il workflow di accesso verso l'accettazione o il rifiuto della richiesta di accesso stessa.

Al fine di tenere traccia delle attività di richiesta di accesso e le relative risposte generate dal sistema, verrà attivato un meccanismo di tracciatura e storicizzazione delle attività relative alle richieste di accesso ai servizi gestiti dalla soluzione.

Il log di tracciatura degli accessi ai servizi conterrà le segnalazioni e tutte le informazioni che la soluzione, di volta in volta, gestisce durante lo svolgimento delle operazioni previste dal workflow di autenticazione e autorizzazione. Le segnalazioni, corredate di tutti gli attributi di dettaglio, verranno raccolte in tempo reale dalle singole componenti della soluzione e inoltrate verso una base dati che si occuperà di raccogliere e storicizzare le informazioni stesse.

Tale operazione avverrà all'interno delle componenti di runtime della soluzione mediante l'utilizzo di una coda di messaggi nella quale saranno scritti tutti i dati relativi all'evento generato, ivi compreso il timestamp del momento in cui si è verificato l'evento. Tale informazione sarà impostata leggendo la data di sistema del server che ospita la componente che ha generato l'evento.

In questo modo si garantisce che nessuna operazione vada persa anche in caso di sovraccarico del sistema e che ciascun evento venga archiviato con il proprio timestamp (data e ora) anche se la scrittura fisica del record fosse differita a causa di carichi particolari del sistema.

Le informazioni di tracciatura così raccolte verranno indirizzate verso file di Log o verso apposite strutture dati preposte per la raccolta dei dati di audit e mantenute per il tempo previsto dalle disposizioni in materia.

Tutte le tracciature così raccolte potranno essere consultate in una delle seguenti modalità:

- Mediante il richiamo di appositi *task* dalla *User Console* della soluzione CA CloudMinder effettuato da parte di un amministratore abilitato o di un utente generico (in self management)
- Visualizzazione della reportistica generata sui dati di *audit* all'interno della *User Console* di CA SiteMinder
- Mediante interrogazione diretta del database di audit della soluzione mediante gli strumenti Client del RDBMS utilizzato o lettura delle informazioni riportate all'interno dei *file* di LOG.

Questi dati saranno quindi utilizzati per ricostruire l'operato della soluzione, effettuare analisi di dettaglio in caso di anomalie della soluzione o, nei casi in cui fosse necessario, dirimere eventuali controversie con terze parti.

10 Gestione del ciclo di vita dell'Identità Digitale

Il servizio di Identity Provider assicura la gestione delle identità attraverso tutto il loro ciclo di vita.

10.1 Visualizzazione attività dell'identità

È disponibile un'area di 'Self Customer Care' del titolare, tramite la quale il titolare di una identità digitale ha la possibilità, accedendo all'interfaccia web del servizio, di visualizzare direttamente le informazioni relative allla propria Identità Digitale.

Sono disponibile le informazioni relative a:

- utilizzo effettivo della propria identità digitale (le ultime Autenticazioni effettuate con successo).

- la documentazione personale e contrattuale sottoscritta digitalmente (Richiesta di Identità digitale SPID, Condizioni Generali di Fornitura e Informativa sulla Privacy) durante le fasi di Registrazione.

Per visualizzare i propri dati il Gestore richiede l'autenticazione almeno al livello 2 SPID (LoA3 dello standard ISO/IEC 29113).

10.2 Modifica dell'identità

10.2.1 Richiesta di modifica degli attributi dell'identità

Il titolare di una identità digitale 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 al livello 2 SPID (LoA3).

10.2.2 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, le corrispondenti Userid verranno inviate 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 fornita al momento della registrazione. In caso di verifica positiva dei dati inseriti, l'utente riceve alla casella fornita e verificata al momento della registrazione una email contenente un link, selezionando il link l'utente riceverà un codice di attivazione password tramite SMS al numero di telefono fornito e verificato in sede di registrazione.

10.2.3 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 90 giorni), il rinnovo e/o la ri-emissione delle credenziali possono essere effettuati utilizzando la stessa procedura di modifica indicata al par. 10.2.2.

10.3 Fornitura dell'identità alle autorità competenti

Il Gestore fornisce le informazioni relative alla identità corrispondenti a un determinato codice univoco oppure corrispondenti a una determinata persona esclusivamente nei casi previsti dalla normativa e in particolare: al titolare legittimo, all'amministrazione di afferenza, all'Autorità Giudiziaria e al Garante della Privacy.

Il Gestore esegue una apposita procedura a garanzia della confidenzialità delle informazioni trasmesse e della verifica della legittimità della richiesta.

10.4 Revoca

Questa sezione descrive il processo di revoca dell'Identità Digitale, specificando le circostanze in cui un'Identità può e deve essere revocata e le modalità in cui la revoca deve essere richiesta, effettuata e notificata al Titolare.

10.4.1 Motivazioni di revoca

Ai sensi della normativa vigente l'Identità Digitale deve essere revocata quando ricorrono una o più delle seguenti circostanze:

- **Richiesta da parte del Titolare**. Il titolare di una identità digitale ha la possibilità di richiedere la revoca della sua identità, secondo le modalità indicate al par. 10.4.2.1. Il gestore procederà tempestivamente con la sospensione cautelativa delle credenziali relative all'identità e verificherà la legittimità della richiesta ricontattando il richiedente. In caso di esito positivo della verifica, revocherà l'identità, comunicando al titolare il completamento e l'esito finale dell'operazione.
- **Sospetti abusi e/o falsificazioni**. Il soggetto titolare di una Identità digitale, 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 via PEC o una richiesta in formato elettronico sottoscritta con firma digitale o elettronica inviata ad un indirizzo di posta dedicato fornito dal gestore. Il gestore provvede a sospendere cautelativamente l'identità digitale disconosciuta e ne dà tempestiva comunicazione. 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 lasciata nello stato di sospensione fino alla sua naturale scadenza.
- **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 del soggetto utente (eredi o procuratore, amministrazione, società subentrante) oppure di una delle autorità competenti. In tal caso il gestore verifica la veridicità del decesso o dell'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**. In caso di scadenza della documentazione di identificazione, 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.

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

- la modifica o la scadenza del rapporto che intercorre tra il Titolare 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 del Titolare è venuto meno;
- riscontro che il Titolare dell'identità digitale 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 un periodo pari a venti anni dalla revoca dell'identità digitale.

10.4.2 Modalità generali ed effetti della revoca

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.

10.4.2.1 Ricezione e verifica di una richiesta di revoca

Il Titolare che intenda revocare la propria identità digitale deve inoltrare richiesta di revoca per iscritto secondo le seguenti modalità:

- Invio tramite PEC alla casella di PEC indicata dal gestore;
- Invio della richiesta in formato elettronico sottoscritta con firma digitale o elettronica del Titolare all'indirizzo di posta elettronica indicato dal gestore;
- Invio della richiesta in formato cartaceo con firma autografa del Titolare corredata da una copia del di un suo documento di identità in corso di validità, all'indirizzo indicato dal gestore.

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

N. B. Se la revoca è motivata da smarrimento o furto degli strumenti per l'uso del servizio, la richiesta dovrà essere accompagnata dalla fotocopia della denuncia di smarrimento o furto.

La richiesta di revoca del Titolare dell'Identità Digitale deve contenere:

1. esplicita dichiarazione della volontà di revocare l'Identità Digitale;
2. motivazione della richiesta di revoca e sua decorrenza;
3. 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.

Il Gestore si riserva il diritto di non procedere alla revoca definitiva dell'identità digitale bensì alla sua sospensione immediata sino alla verifica della correttezza formale della richiesta di revoca.

In qualunque caso, qualora il Titolare intenda inoltrare una **richiesta di revoca immediata**, tale volontà deve essere riportata esplicitamente**.** Sono comunque considerate tali quelle che adducono esplicitamente una delle motivazioni seguenti:

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

10.4.2.2 Attuazione della Revoca

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'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).

10.4.2.3 Notifica al Titolare

L'avvenuta revoca di una Identità Digitale viene notificata al Titolare tramite l'indirizzo di posta elettronica dichiarato dal titolare in fase di registrazione.

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

10.4.2.3.1 Notifica anticipata

Secondo quanto previsto dalla normativa vigente, l'intenzione di revocare una identità digitale è notificata anticipatamente al Titolare, 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 del Titolare 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.

10.5 Sospensione

Questa sezione descrive il processo di sospensione dell'identità digitale, specificando le circostanze in cui un'Identità può essere sospesa e le modalità in cui la sospensione deve essere richiesta, effettuata e notificata al Titolare.

10.5.1 Motivazioni e modalità di sospensione

La sospensione dell'identità digitale può essere effettuata nei casi e dai soggetti seguenti:

- su **richiesta del Titolare**;
- su **richiesta dell'Incaricato**;
- su **iniziativa del Gestore**.

La ***sospensione su richiesta del Titolare*** 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 ad un indirizzo di posta elettronica certificata del Gestore,
- richiesta inviata in formato cartaceo con firma autografa e fotocopia del documento di identità del titolare in corso di validità (oppure fotocopia della denuncia di suo smarrimento o furto), via posta ordinaria all'indirizzo della sede del Gestore,

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

La ***sospensione su richiesta 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 ad un indirizzo di posta elettronica certificata del Gestore,
- richiesta inviata in formato cartaceo con firma autografa e fotocopia del documento di identità del titolare in corso di validità (oppure fotocopia della denuncia di suo smarrimento o furto), via posta ordinaria all'indirizzo della sede del Gestore,

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

I **casi di emergenza** in cui il Titolare 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).

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.

10.5.1.1 Ricezione e verifica di una richiesta di sospensione

Il Titolare o un Incaricato che intenda ottenere la sospensione di una identità digitale deve inoltrare regolare richiesta di sospensione secondo le modalità descritte nel presente paragrafo.

Il Gestore effettua la sospensione non appena riceve la richiesta.

Nella richiesta di sospensione per iscritto devono essere chiaramente indicati:

- esplicita dichiarazione della volontà di sospendere l'identità digitale (se la richiesta proviene dal Titolare);
- la motivazione della richiesta di sospensione;
- i seguenti dati anagrafici del Titolare 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 previsti al par. 10.5.1.

10.5.1.2 Ricezione e verifica di una richiesta di sospensione telefonica

Il Titolare che intenda procedere con la Sospensione Telefonica della propria Identità Digitale deve contattare l'Help Desk dedicato e seguire la procedura indicata dall'Operatore dell'Help Desk e descritta in questo paragrafo.

Nella fattispecie, nel caso di sospensione richiesta telefonicamente al numero verde dedicato all'Help Desk, la procedura che è la seguente:

- L'Utente contatta il numero verde 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 a seconda della disponibilità – da parte dell'utente – di telefono cellulare e/o e-mail, dichiarati dal richiedente 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 e-mail:
  - L'Operatore dell'Help Desk invia un codice "*one-shot*" all'indirizzo e-mail utilizzando le funzionalità messe a disposizione dal Portale del Gestore (l'operatore di Help Desk non ha visibilità dell'e-mail inviata),
  - L'Utente fornisce telefonicamente all'operatore di Help Desk il codice "*one-shot*" ricevuto via e-mail,
  - 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.

10.5.1.3 Attuazione della sospensione

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, qualora non riceva richiesta formale di revoca, il gestore lascia l'identità digitale nello stato di sospesafino alla sua naturale scadenza.

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).

10.5.1.4 Notifica al Titolare

L'avvenuta sospensione di una identità digitale viene notificata al Titolare tramite l'indirizzo di posta elettronica dichiarato dal titolare in fase di registrazione.

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

10.5.1.4.1 Notifica anticipata

Secondo quanto previsto dalla normativa vigente, l'intenzione di sospendere una identità digitale è notificata anticipatamente al Titolare, salvo casi di motivata urgenza, ogni qual volta la sospensione avvenga per iniziativa del Gestore o terzo interessato.

In ciascun caso, la notifica contiene:

- i dati identificativi univoci del Titolare 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 il certificato non è più valido.

10.6 Riattivazione

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

10.6.1 Motivazioni e modalità di riattivazione

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

- su **richiesta del Titolare;**
- su **richiesta dell'Incaricato**;
- su **iniziativa del Gestore.**

10.6.1.1 Ricezione e verifica di una richiesta di riattivazione

Le richieste di **riattivazione da parte del Titolare** dovranno essere inoltrate nelle seguenti modalità:

- 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 del Gestore,
- richiesta inviata, in formato cartaceo con firma autografa e fotocopia del documento di identità del Titolare in corso di validità (oppure fotocopia della denuncia di suo smarrimento o furto), via posta ordinaria all'indirizzo della sede del Gestore,

Per le ultime due 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, ove richiesta nei casi precedentemente descritti.

Nel caso in cui l'Identità digitale sia stata sospesa su decisione 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** possono essere inoltrate via e-mail e devono contenere:

- esplicita dichiarazione della volontà di riattivare l'identità digitale;
- la motivazione della riattivazione e la decorrenza richiesta;
- i seguenti dati anagrafici del Titolare:
  - 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, ove richiesta nei casi precedentemente descritti.

10.6.1.2 Attuazione della riattivazione

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.

Il Gestore garantisce la tempestiva esecuzione della riattivazione in questione.

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).

10.6.1.3 Notifica al Titolare

La riattivazione di un certificato viene notificata al Titolare tramite l'indirizzo di posta elettronica dichiarato dal titolare in fase di registrazione.

10.6.1.3.1 Notifica anticipata

L'intenzione di riattivare una identità è notificata anticipatamente al Titolare, salvo casi di motivata urgenza, ogni qual volta la richiesta provenga da un terzo interessato.

In ciascun caso, la notifica contiene:

- i dati identificativi univoci del Titolare 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.

11 Sincronizzazione Temporale dei Sistemi del Gestore

Il Gestore in qualità di Certificatore Accreditato per la firma elettronica qualificata dispone di un sistema di riferimento temporale che garantisce il funzionamento di tutti i suoi servizi in conformità ai requisiti previsti dalla normativa in vigore. Il Gestore garantisce tramite questo proprio sistema il livello di accuratezza temporale richiesto dalla normativa SPID per tutti i server utilizzati nella piattaforma di erogazione del servizio.

Personale espressamente autorizzato dal Gestore provvede al buon funzionamento del sistema di sincronizzazione temporale.

La soluzione *CA CloudMinder* è dotata di un sistema di registrazione di tutti gli eventi correlati con l'operatività delle sue componenti di run-time di front e back-end. Questa gestione della registrazione degli eventi rende quindi possibile la fruizione in tempo reale delle notifiche di stato di tutte le componenti (servizi e/o processi) in esecuzione e delle informazioni che, a seconda del livello di dettaglio prescelto in fase di configurazione (*Information, Warning, Error, Debug, etc*), si deciderà di propagare sui file di log o verso gli archivi di Audit e Reporting.

La soluzione si avvale di un meccanismo di logging che sfrutta un sistema di gestione delle code (JMS ad esempio) per propagare le informazioni sugli eventi verso un archivio fisico in un formato standard. Questo formato prevede sempre un campo di riferimento temporale (ottenute dal sistema operativo nel momento in cui la componente interessata intercetta l'evento da tracciare), un codice di errore (se esiste nel caso specifico), una *severity* e una descrizione dell'anomalia riscontrata o della segnalazione. La corrispondenza dell'orario effettivo dell'evento con quello indicato nel file di log è assicurata dal meccanismo di code che consente alla soluzione di riportare informazioni corrette e tempestive sui log anche se, per questioni di particolare carico straordinario, la scrittura avvenisse in modalità differita a livello temporale.

12 Privacy e Protezione dei dati personali

In considerazione della grande importanza attribuita al proprio interno alla tematica del trattamento dei dati personali, nell'ambito del Gruppo Telecom Italia è operativo un sistema organizzativo e normativo interno per garantire che tutti i trattamenti di dati personali si svolgano nel rispetto delle disposizioni di legge vigenti e dei principi di correttezza e liceità dichiarati nel Codice Etico del Gruppo. Il complesso delle misure previste e messe in atto dal sistema implementato nel Gruppo Telecom Italia incorporano anche le misure minime previste dalla [Normativa Privacy].

Tale sistema si caratterizza per alcune importanti elementi di base, fra i quali si ricordano i seguenti:

- i dipendenti che hanno ricevuto la nomina di Incaricati ai sensi della [Normativa Privacy], hanno ricevuto dettagliate istruzioni circa le modalità e le misure di sicurezza da adottare per il trattamento dei dati personali;
- il trattamento dei dati personali avviene sotto la supervisione di responsabili del trattamento, anch'essi formalmente nominati, i quali hanno a loro volta ricevuto le necessarie istruzioni ed indicazioni operative;
- apposite funzioni aziendali hanno il compito di definire le policy per la sicurezza delle informazioni e di verificare, con l'ausilio di funzioni di auditing interno, che esse siano effettivamente applicate;
- il sistema di policy si basa sulla corretta classificazione degli asset. Con l'ausilio di strumenti di risk assessment, sono individuate le misure di sicurezza più idonee alla tutela dei singoli asset, alla definizione dei controlli e all'applicazione dei sistemi di monitoraggio e verifica più appropriati;
- la tutela dei dati personali non si configura come un processo indipendente, ma risulta del tutto integrato nella gestione corrente della sicurezza degli asset aziendali;
- le politiche di sicurezza fisica e di tutela del patrimonio materiale dell'azienda e le politiche di gestione degli incidenti di sicurezza e delle crisi sono definite tenendo presenti i principi di tutela dei dati personali e le necessità di protezione di questi dati fissate dalla legge.

Nell'ambito delle policy di sicurezza aziendale sono state sviluppate soluzioni tecniche ed organizzative per la protezione dei dati trasmessi e conservati sulla rete e sui sistemi aziendali, fra cui rientrano, a titolo esemplificativo e non esaustivo:

- protezione dai virus con aggiornamento continuo;
- hardening dei sistemi utilizzati;
- software distribution per l'aggiornamento automatico delle patch di sicurezza sui sistemi aziendali;
- tool e metodologie di vulnerability assessment e risk analisys;
- protezione informatica e dei punti di accesso alla rete aziendale (ad esempio: Controllo Accessi, Credenziali di autenticazione, ecc.);
- partizionamento e protezione delle reti interne;
- monitoraggio della rete e dei sistemi per la prevenzione ed il contrasto degli incidenti di sicurezza.

I dati personali sono trattati, conservati e protetti dal Gestore conformemente a quanto previsto dalla [Normativa 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.

13 Riferimenti

13.1 Riferimenti Normativi

Il servizio offerto dal Gestore è conforme al quadro normativo sintetizzato nella tabella di seguito indicata, nella quale si riportano le abbreviazioni utilizzate nel testo del presente Manuale Operativo per riferimento alle singole norme.

SIGLA	DESCRIZIONE
[CAD]	**CAD, Decreto Legislativo 7 marzo 2005**, n. 82 Codice dell'amministrazione digitale.
[DL 159/2006]	**Decreto Legislativo 4 aprile 2006, n. 159** – Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.
[DPCM 2009]	**Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 – Regole tecniche in materia di firme digitali** – Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici (Gazzetta Ufficiale n. 129 del 6 giugno 2009).
[EIDAS]	**EIDAS, Regolamento UE N. 910/2014** del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
[DPCM SPID]	**DPCM 24 ottobre 2014** "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese". Pubblicato nella Gazzetta Ufficiale n.285 del 9122014.
[DPR 194/14]	**Decreto del Presidente del Consiglio dei Ministri 10 novembre 2014, n. 194**, Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente.
[AGID 44/2015]	**Determinazione AGID N. 44/2015, del 28 luglio 2015**, relativa all'emanazione dei regolamenti SPID di cui all'art l'Art. 4 commi 2,3 e 4 del DPCM 24 ottobre 2014 recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese." Pubblicato sulla GU Serie Generale n.285 del 9 dicembre 2014.
[RegoleTecniche]	**Regolamento AGID del 28 luglio 2015**, recante le regole tecniche (articolo 4, comma 2, DPCM 24 ottobre 2014)
[Procedure]	**Regolamento AGID 28 luglio 2015**, recante le procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale ai sensi del DPCM 24 ottobre 2014
[Regolamento Identità Pregresse]	**Regolamento AGID 28 luglio 2015,** Recante le procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale ai sensi del DPCM 24 ottobre 2014
[AGID 40/2016]	**Determinazione AGID N. 40/2016, del 23 febbraio 2016**, relativa alla "emanazione schema convenzione, con le integrazioni proposte dal Garante per i dati personali, tra l'Agenzia per l'Italia Digitale e le pubbliche amministrazioni in qualità di fornitori di servizi

	in materia di Sistema Pubblico per la gestione dell'identità digitale di cittadini e imprese". Pubblicato sulla GU Serie Generale n.44 del 23 febbraio 2016.
[Accreditamento 2.0]	**Regolamento AGID versione 2.0 del 22 luglio 2016** recante le modalità per l'accreditamento e la vigilanza dei Gestori dell'Identità Digitale (articolo 1, comma 1, lettera l) , DPCM 24 ottobre 2014),
[Modalità Attuative 2.0]	**Regolamento AGID versione 2.0 del 22 luglio 2016**, recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014)
[Normativa Privacy]	**Regolamento 2016/679/UE (Regolamento generale sulla protezione dei dati – di seguito GDPR) e dell'articolo 122 del Codice in materia di protezione dei dati personali (D.Lgs. 196/03, il c.d. Codice privacy).**

Inoltre, avuto riguardo allo status di Gestore di Pubblico Servizio che assume TI Trust Technologies nella propria attività di Gestore delle Identità Digitale SPID ([DPCM SPID] art. 1), a completamento del quadro normativo delineato ed ancorché non specificamente richiamate nel testo del presente documento, trovano ulteriore applicazione le normative di seguito indicate, per le componenti applicabili a SPID, ai soggetti da essi previsti ed ai ruoli e alle attività da questi esercitati:

- Disciplina sulla responsabilità da contatto sociale qualificato in relazione alla qualità e continuità dei servizi come da Convenzione con la PA
- Obblighi civilistici di parità di trattamento e non discriminazione nell'accesso al servizio e nell'erogazione del medesimo
- Norme sul trattamento dei dati personali
- Disciplina sull'autocertificazione, in particolare ex art. 15 della legge 12 novembre 2011, n. 183
- Commissariamento in luogo dell'interdizione ai sensi dell'art. 15 del D. Lgs. n. 231/2001 in tema di responsabilità amministrativa degli enti dipendente da reato
- Disciplina dell'ineleggibilità di amministratori e legali rappresentanti ex art. 10, dPR n. 361/1957
- Obbligo di denuncia ex art. 331 cpp
- Disposizioni in tema di reati propri.

Nell'ambito di queste disposizioni, non trovano applicazione in relazione alla natura di soggetto interamente privato di TI Trust Technolgies le disposizioni seguenti:

- Regole di evidenza pubblica ex Codice dei Contratti Pubblici
- Legge 241/1990 e disciplina sull'accesso agli atti
- Obblighi pubblicitari e di trasparenza ex art 1, comma 34, legge anticorruzione n. 190/2012

13.2 Standard di riferimento

[1] ISO/IEC 18014 Time-stamping
[2] ISO/IEC 19790:2012 Security requirements for cryptographic modules
[3] ISO/IEC 24760-1 A framework for identity management - Part 1: Terminology and concept
[4] ISO/IEC 15408-1 Evaluation criteria for IT security - Part 1: Introduction and general model
[5] ISO/IEC 27001 Information security management
[6] ISO/IEC 29003 Identity proofing
[7] ISO/IEC 29100 Basic privacy requirements
[8] ISO/IEC 29115:2013 Entity authentication assurance framework
[9] ITU-T X.1254 Entity Authentication Framework
[10] ITU-T Recommendation X.1252 (2010) Baseline identity management terms and definitions
[11] NIST 800-63-2 Electronic Authentication Guideline
[12] FIPS PUB 140-2 Security requirements for cryptographic modules

14 Definizioni

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale Operativo, i termini e le espressioni sotto elencate avranno il significato descritto nella definizione riportata. Le definizioni adottate dalla normativa di riferimento non sono riportate e si rimanda ai testi in vigore per la loro consultazione. I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene. Dove appropriato viene indicato anche il termine inglese corrispondente, generalmente usato in letteratura tecnica e negli standard.

Adesione: è il primo passaggio del processo di iscrizione, dove una entità aderisce a SPID fornendo tutti i dati e la documentazione necessaria.

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

Attributi secondari: il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni.

Autenticazione: disposizione di garanzia sull'identità dell'entità (ISO-IEC 18014-2).

Autenticazione multi-fattore: autenticazione con almeno due fattori di autenticazione indipendenti (ISO-IEC 19790).

Centro Servizi del Gestore: La struttura logistica del Gestore in cui vengono eseguite le principali operazioni relative all'erogazione del servizio. Tale struttura è protetta secondo avanzati standard di sicurezza logica e fisica, come dettagliatamente riportato nel Piano per la Sicurezza del Gestore.

Cifratura: La trascrizione di un'evidenza informatica secondo un codice riservato che la renda inintelligibile ai terzi. Le operazioni di cifratura e decifrazione si effettuano applicando algoritmi standard che prevedono l'utilizzo di chiavi segrete.

Cliente: soggetto, persona fisica o giuridica, o Ente o Pubblica Amministrazione che sigla il contratto di fornitura con il Gestore, relativo alla fornitura del servizio di Identità Digitale.

Codice identificativo: il particolare attributo assegnato dal gestore dell'identità' digitale che consente di individuare univocamente un'identità digitale nell'ambito dello SPID.

Credenziale: un insieme di dati presentati come evidenza dell'identità dichiarata/asserita o di un proprio diritto (ITU-T X.1252), in pratica il Titolare/utente si avvale di questo attributo (a singolo o doppio fattore) unitamente al codice identificativo (entrambi rilasciati dal gestore dell'identità digitale) per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi (Amministrazioni e privati) che aderiscono allo SPID.

Elenco pubblico dei Gestori Accreditati: registro, tenuto dall'Agenzia per l'Italia Digitale, accessibile al pubblico, contenente l'elenco dei soggetti abilitati ad operare in qualità di gestori dell'identità digitale.

Entità: può essere una persona fisica o un soggetto giuridico.

Fattore di autenticazione: elemento di informazione e/o processo usato per autenticare o verificare l'identità di una entità (ISO-IEC 19790).

Firma Elettronica: è l'insieme di dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzati dal firmatario per firmare.

Firma Elettronica Avanzata: è una firma elettronica che soddisfa i seguenti requisiti: (i) è connessa unicamente al firmatario, (ii) è idonea ad identificare il firmatario, (iii) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo, (iv) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Fonte Autoritativa: in generale un repository riconosciuto come sorgente aggiornata ed accurata delle informazioni (ISO-IEC 29003).

Fornitore di servizi: il fornitore dei servizi della società dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al gestore dell'identità digitale che l'ha fornita.

Gestori dell'identità digitale (Gestore, Identity Provider, IDP): prestatore di servizi di gestione dell'Identità Digitale, la società TI Trust Technologies, che eroga tale servizio in conformità alla normativa.

Identità digitale: la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale.

Incaricato: la persona fisica o giuridica cui il gestore conferisce l'incarico di effettuare per suo conto, sotto la sua responsabilità, attenendosi alle istruzioni da lui stesso impartite ed utilizzando gli strumenti da lui stesso indicati, l'operazione di identificazione e di registrazione dei Titolari. L'Incaricato in alcuni casi è anche responsabile della consegna delle credenziali, o dei mezzi per produrre le credenziali.

Indice Nazionale delle Anagrafi (INA): il sistema del Ministero dell'Interno, Centro Nazionale per i Servizi Demografici di cui all'articolo 2-quater del Decreto Legge n. 392, del 27 dicembre 2000, convertito, con modificazioni, dalla legge 28 febbraio 2001, n. 26. L'INA contiene, per ogni cittadino residente in Italia, le informazioni seguenti (validate dal Comune per la parte anagrafica e la residenza e dall'Agenzia delle Entrate per quanto riguarda il codice fiscale): codice fiscale, cognome, nome, sesso, data di nascita, codice del comune di nascita, codice del comune di residenza, data di eventuale decesso.

Manuale Operativo: il documento pubblico che definisce le modalità operative del servizio di identity provider.

Manuale della Qualità: il manuale predisposto dal Gestore per ottenere la certificazione di qualità ISO 9001, come previsto dalla normativa vigente.

OTP: una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione.

Piano della Sicurezza: il documento che definisce le modalità di gestione delle attività connesse alla protezione e conservazione di dati, programmi ed apparati del Gestore. Tale documento, che contiene informazioni riservate, non è divulgato pubblicamente ma depositato presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione, a garanzia della sua completezza e conformità a quanto previsto dalla normativa vigente e dagli attuali standard internazionali di sicurezza (art. 31 del DPCM 2009).

Protocollo di autenticazione: sequenza definita di messaggi fra una entità e il verificatore allo scopo di consentire al verificatore di autenticare l'entità.

Pubbliche Amministrazioni: le amministrazioni di cui all'articolo 1, comma 2, ed all'articolo 70, comma 4, del decreto legislativo 30 marzo 2001, n. 165.

Richiedente: è la persona fisica che effettua l'adesione. Se la persona fisica non è l'entità (v. soggetto giuridico), essa deve avere titolarità o procure per agire per conto dell'entità.

Registrazione: il processo che, partendo dall'iniziale adesione e a seguito delle fasi di dimostrazione e validazione, si completa con la registrazione con esito positivo della nuova identità digitale e con il rilascio delle credenziali. (ISO-IEC 29003).
Smartcard: dispositivo elettronico costituito da un microchip inserito in una tessera di plastica delle dimensioni di una carta di credito. Il microchip è programmabile, può contenere dati e applicativi e interagire con altre apparecchiature elettroniche e computer tramite un apposito lettore.

SPID: il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98.

Titolare: è il soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SPID, corrisponde all'utente del DPCM art. 1 comma 1 lettera v).

Verificatore: il soggetto attore, nel caso SPID il gestore delle identità digitali, che conferma e avvalora le informazioni di identità.

15 Acronimi

AgID (Agenzia per l'Italia Digitale, ex DigitPA). L'articolo 20, comma 2, della legge 134/2012 attribuisce all'Agenzia lo svolgimento delle funzioni di coordinamento, di indirizzo e regolazione precedentemente affidate a DigitPA, nonché l'emanazione di pareri obbligatori sugli schemi di contratto concernenti l'acquisizione di beni e servizi informatici e telematici, secondo quanto previsto dall'articolo 3 del D.lgs. n. 177/2009. In forza del quadro normativo citato, in particolare vengono attribuite all'Agenzia anche le funzioni di consulenza e proposta, (già previste nell'articolo 3, comma 2, lettera a) del citato del D.lgs. 177/2009) nonché l'emissione di valutazioni e pareri facoltativi (secondo quanto previsto dal citato articolo 3, comma 2 lettera c) del D.lgs177/2009 e dall'articolo 20, comma 3 lettera l) della legge 134/2012).

DPCM SPID – DPCM del 24 ottobre 2014 (pubblicato in GU Serie Generale n.285 del 9-12-2014) in cui si definiscono le Caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.

ETSI – European Telecommunications Standards Institute.

FEA – Firma Elettronica Avanzata.

HTTP (HyperText Transfer Protocol): Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web.

HTTPS (Secure HyperText Transfer Protocol): Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifrazione dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad una estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL.

IDP – Identity Provider (il gestore delle identità digitali in ambito SPID).

IEEE – Institute of Electrical and Electronics Engineers.

INTERNET – Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. La sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW).

ISO – **International Standards Organization**: Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell' area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO.

ITSEC – **Information Technology Security Evaluation Criteria**: Criteri europei per la valutazione della sicurezza nei sistemi informatici.

ITU-T – International Telecommunication Union, Telecommunication Standardization Sector

LoA – Level of Assurance

PIN – Personal Identification Number

PKCS – Public Key Cryptography Standard.

SAML – Security Assertion Markup Language.

SFTP – **Secure File Transfer Protocol**: protocollo di rete che prevede il trasferimento sicuro dei dati e funzionalità di manipolazione.

SIAV – Sistema di Identificazione tramite registrazione Audio-Video.

SLA – **Service Level Agreement**: misurano la rispondenza di un servizio a quanto stabilito contrattualmente.

SSL – Secure Socket Layer.

TCP – **Transmission Control Protocol**

TLS – **Transport Layer Security**

TITT – Telecom Italia Trust Technologies S.r.l.

TI – Telecom Italia

URL – Uniform Resource Location

XML – eXtensible Markup Language: linguaggio marcatore basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo.