

CONDIZIONI GENERALI PER L'USO DEI SERVIZI EROGATI DA SIELTE S.P.A.

1. Premesse

L'erogazione del servizio di identità digitale (IdP) è regolata da un'apposita normativa e da specifiche tecniche emanate da AgID – Agenzia per l'Italia Digitale.

Il servizio di IdP può essere fornito solamente da prestatori di identità digitali accreditati e iscritti al registro pubblico tenuto dall'AgID – Agenzia per l'Italia Digitale, presso il quale SIELTE risulta iscritta in qualità di IDP (Identity Provider).

2. Definizioni

Il servizio di Identity Provider consiste nella gestione e verifica dell'identità degli utenti che operano sui siti web della pubblica amministrazione che fanno uso dei meccanismi di autenticazione e autorizzazione progettati all'interno di SPID.

Nell'ambito del sistema SPID vengono individuati i seguenti soggetti:

- **GESTORE IDENTITÀ DIGITALE** (detto Identity Provider) – gestisce le identità digitali e provvede a tutti i meccanismi di autenticazione e autorizzazione di un utente;
- **FORNITORE DEI SERVIZI** (detto Service Provider) – fa uso del gestore dell'identità digitale (IdP) per autenticare e autorizzare l'accesso agli utenti, detti User Agent (UAs), alle proprie aree dei servizi riservati;
- **UTENTE** (detto User Agent) – richiede e dispone di una o più identità digitali, che contengono le informazioni necessarie all'identificazione da parte del fornitore di servizi (Service Provider), come ad esempio il sito dell'agenzia delle entrate o quello dell'INPS;

3. Oggetto del servizio

L'UTENTE richiede a SIELTE la gestione della propria identità digitale secondo la normativa presente nel DPCM del 24 Ottobre 2014.

4. Modalità per accedere al servizio

L'UTENTE, a fronte di un regolare contratto attivo, richiede l'attivazione del servizio di Identità Digitale tramite il portale di SIELTE.

Due diverse tipologie di servizio sono state previste:

- **Livello 1:** garantisce con un buon grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio moderato e compatibile con l'impiego di un sistema autenticazione a singolo fattore, ad es. la password; questo livello può essere considerato applicabile 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:** garantisce con un alto grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio ragguardevole e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell'identità digitale può provocare un danno consistente;

SIELTE, per ciascun livello di servizio garantito, si attiva verso un referente tecnico aziendale (di seguito Identity

Manager), che provvede al riconoscimento e alla identificazione dell'UTENTE attraverso procedure di indagine che ne verificano la corretta Identità.

5. Modalità di erogazione del servizio

Attraverso l'adozione di una metodologia standard, all'UTENTE saranno sottoposte delle fasi per la corretta identificazione e per il rilascio delle credenziali associate all'identità digitale

I singoli ed eventuali problemi segnalati dall'UTENTE vengono prese in carico dagli specialisti di SIELTE in base ad una pianificazione standardizzata delle attività di analisi e delivery.

SIELTE si riserva la facoltà di affidare, in tutto o in parte, le prestazioni di cui al presente servizio a ditte specializzate e da essa stessa autorizzate, interne e/o esterne alla propria organizzazione.

6. Limitazioni al servizio ed esclusioni

Il presente servizio non comprende:

- a. Qualsiasi attività di aggiornamento software, di tipo migliorativo e/o di adeguamento alle modifiche legislative e/o orientata allo sviluppo di implementazioni di qualsivoglia tipo, intendendosi con tale concetto la progettazione, creazione, modifica e/o inserimento di novità nei programmi software rilasciati.
- b. Qualsiasi intervento che eventualmente si rendesse necessario presso la sede dell'UTENTE (on-site) e comunque tutte le attività di addestramento, di installazione, di analisi, di consulenza, di sviluppo software e di modifica, oltre a quelle indicate nel servizio scelto.
- c. Le attività per il ripristino dei programmi e/o dei dati dovute a perdita totale o parziale degli stessi, indipendentemente dalle cause dirette o indirette che abbiano determinato tale perdita.
- d. La sistemazione di anomalie nei dati, sia che queste derivino da guasti provocati dal software sia da errori degli operatori.
- e. Tutto quanto non espressamente indicato ai punti 4 e 5.

SIELTE si riserva la facoltà di escludere l'UTENTE dall'accesso ai servizi o di prendere le misure che riterrà opportune nel caso in cui l'UTENTE non osservi le norme definite e le condizioni standard di utilizzo dei servizi stessi.

7. Obblighi e responsabilità di SIELTE

Gli obblighi di SIELTE sono solo quelli che derivano dagli impegni assunti indicati nel presente documento. Salvo i casi di dolo o colpa grave, SIELTE non assume responsabilità alcuna per danni diretti o indiretti, incidentali o consequenziali, eventualmente provocati all'UTENTE, nell'erogazione dei servizi descritti nel presente servizio. In ogni caso la responsabilità SIELTE sarà sempre limitata ad un importo massimo pari a quello pagato dall'UTENTE a SIELTE per la specifica prestazione che ha provocato il fatto contestato.

8. Obblighi e responsabilità dell'UTENTE

L'UTENTE non potrà cedere ad altri il presente accordo di servizio senza il preventivo consenso scritto di SIELTE.

Rientrano nell'esclusiva responsabilità dell'UTENTE la predisposizione in stato di sicurezza degli archivi dei dati da elaborare, la supervisione, la direzione ed il controllo dell'uso delle procedure ed in genere tutte le operazioni connesse e/o strumentali a tale uso.

In particolare appartiene all'esclusiva competenza e responsabilità dell'UTENTE

- a) Porre in essere le procedure necessarie a salvaguardare l'integrità e la sicurezza dei dati e dei programmi rispetto ad accessi ed utilizzazioni autorizzati e/o non autorizzati ed a ricostruire dati corrotti o alterati a seguito di non corretto uso delle procedure;

L'UTENTE in ogni caso concorda di sollevare SIELTE da qualsiasi responsabilità per danni diretti o indiretti derivanti da smarrimento e/o distruzione di dati, per guasti nelle procedure, vizi nella documentazione o per anomalie ed errori. Eventuali operazioni di ripristino straordinarie derivate dalla indisponibilità di backup o dalla inadeguatezza degli stessi saranno, indipendentemente dal loro esito, integralmente addebitate all'UTENTE anche se il danneggiamento è stato originato da un intervento di SIELTE.

Nel caso in cui i programmi software forniti vengano in qualche modo modificati e/o manomessi dall'UTENTE o da terzi, l'UTENTE perde il diritto ai servizi di cui al presente servizio.

9. Revoca dell'Identità Digitale

Sono causa di revoca su richiesta dell'UTENTE dell'Identità Digitale:

- Lo smarrimento od il furto delle credenziali di accesso all'identità digitale;
- Lo smarrimento della SIM con il numero di telefono associato per la ricezione degli SMS

Sono causa di revoca dell'identità digitale su iniziativa di SIELTE:

- Il riscontro che l'identità digitale NON è stata rilasciata secondo la vigente normativa ed il MANUALE OPERATIVO;
- Il riscontro che uno dei requisiti per l'accettazione della registrazione dell'UTENTE è venuto meno;
- La sopravvenuta modifica dei dati personali dell'UTENTE o di altri elementi riportati nell'identità digitale;

L'elencazione di cui ai precedenti commi deve ritenersi indicativa, rinviandosi al MANUALE OPERATIVO per l'individuazione di ulteriori fattispecie, nonché per le modalità di comunicazione dell'esercizio del diritto di revoca.

SIELTE, nel pieno rispetto della normativa vigente, si riserva la facoltà di procedere alla revoca dell'identità digitale in quei casi in cui, a proprio insindacabile giudizio, ritenesse venute meno le condizioni di sicurezza per l'espletamento dell'attività di Identity Provider.

10. Sospensione dell'Identità Digitale

SIELTE utilizza in via cautelativa lo strumento della sospensione qualora una richiesta di revoca venga effettuata tramite il canale di comunicazione sicuro fra SIELTE e l'UTENTE riportate nel MANUALE OPERATIVO. In tal caso, le credenziali e/o l'Identità digitale viene SOSPESO temporaneamente. La revoca definitiva viene effettuata solo dopo la ricezione della conferma da parte dell'UTENTE.

LA sospensione può essere effettuata anche su richiesta dell'UTENTE oppure su iniziativa di SIELTE, con le modalità riportate nel MANUALE OPERATIVO.

11. Risoluzione del servizio

L'UTENTE nel caso in cui SIELTE rinunci ripetutamente a fornire il servizio secondo le modalità ed i termini descritti, può richiederne la risoluzione rinunciando fin d'ora a chiedere il risarcimento di eventuali ulteriori danni.

12. Forza Maggiore

SIELTE non è responsabile della mancata osservanza dei propri obblighi o di ritardi se imputabili a cause di forza maggiore, intese come ogni causa fuori dal proprio ragionevole potere di controllo.

13. Foro Competente

Per ogni controversia inerente le presenti condizioni generali è competente in via esclusiva il foro di Roma.