GUIDA UTENTE

Servizio di Gestione Sistema Pubblico dell'Identità Digitale (SPID)

STATO DELLE REVISIONI DELLA GUIDA UTENTE

REV.	CAP.	DESCRIZIONE MOTIVO	DATA
00	TUTTI	EMISSIONE GUIDA UTENTE	11/2015
01	TUTTI	AGGIORNAMENTO GUIDA UTENTE	04/2016
02	4, 6	MODIFICHE AL PROCESSO DI REGISTRAZIONE E GESTIONE DELL'IDENTITA' DIGITALE	09/2016
03	6	AGGIUNTA DESCRIZIONE DELL'APP MYSIELTEID	03/2017
04	6	AGGIUNTO NUOVO PROFILO E SVILUPPO SU UNIVERSAL WINDOWS PLATFORM	05/2017
05	6, 7	SERVIZI ABILITATI A SPID; APP MYSIELTEID: OTP RICEVUTO VIA SMS, IMPRONTA DIGITALE SU ANDROID E RICHIESTA DI SUPPORTO	06/2017
06	4.1, 7, 8	MODIFICA DOCUMENTI IN REGISTRAZIONE; MODIFICA DATI DOMICILIAZIONE E CONSENSO AL TRATTAMENTO DEI DATI; ACCESSI SPID E RESTYLING APP MYSIELTEID	10/2017
07	TUTTI	INSERIMENTO DOCUMENTAZIONE CONSULTABILE DA PROFILO; INSERIMENTO OPERAZIONI PROFILO E DOCUMENTAZIONE SU APP MYSIELTEID; PROCEDURE DI RECUPERO PASSWORD E MODIFICA DOMANDA SEGRETA; GESTIONE IMPRESE E MULTI UTENZA SU APP MYSIELTEID; GESTIONE CREDENZIALI DI LIVELLO 1 E 2; REVISIONE GENERALE DEL DOCUMENTO	04/2018
08	4.1, 7.6, 7.3.1.11	REINGEGNERIZZAZIONE REGISTRAZIONE; RINNOVO IDENTITÀ, NOTIFICHE	10/2018
09	4.1.1.1 4.1.1.2	INSERIMENTO REGISTRAZIONE IDENTITÀ PREGRESSA E REGISTRAZIONE IDENTITÀ PREGRESSA CON MIGRAZIONE ASSISTITA	11/2018
09.1	TUTTI	MODIFICA NUMERO DEL CONTACT CENTER E PROCESSO RECUPERO PASSWORD	09/2019
09.2	7.6 9	REVISIONE PARAGRAFO RINNOVO IDENTITÀ REVISIONE PROCESSO RECUPERO PASSWORD	02/2020

10	4 7.3	INSERIMENTO NUOVA MODALITÀ DI RILASCIO IDENTITÀ DIGITALE CON CIE 3.0, INSERIMENTO SPID LIV 3, MODIFICHE AL CAPITOLO SU REGISTRAZIONE E IDENTIFICAZIONE SIELTEID	03/2020

Sommario

1 Introduzione

1.1 Scopo del documento

Questo documento, denominato “Guida Utente”, contiene le istruzioni per gli utenti che vogliono richiedere, attivare ed utilizzare il servizio SielteID per ricevere le credenziali SPID ed accedere ai servizi online della Pubblica Amministrazione.

Il servizio SielteID è fornito da Sielte S.p.A., in qualità di Identity Provider aderente al Sistema Pubblico per la gestione dell’Identità Digitale, conforme ai sensi del DPCM del 24 ottobre 2014, del CAD e del DPR n. 445.

1.2 Convenzioni di lettura

Nel resto del documento, l’azienda Sielte S.p.A., erogatrice del servizio di gestore dell’identità digitale qui descritto e disciplinato, è indicata semplicemente con “Sielte”.

I riferimenti alla normativa e agli standard sono riportati tra parentesi quadre.

Affinché vengano rispettati i parametri RID previsti dalla norma UNI EN ISO 27001:2013, la distribuzione dei documenti prodotti da Sielte S.p.A. è controllata; i documenti e le loro successive emissioni vengono comunicate ai fruitori autorizzati, poiché direttamente coinvolti nelle attività oggetto dei documenti.

In questo specifico caso, essendo il documento classificato in ambito di riservatezza come “Pubblico”, esso deve essere reso disponibile a tutti. Nel momento in cui il presente documento viene distribuito al di fuori del contesto aziendale, Sielte S.p.A. non è più responsabile del monitoraggio delle copie distribuite.

1.3 Definizioni ed acronimi

AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
CODICE/CODICE DELLA PRIVACY	Codice in materia di protezione dei dati personali
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
GDPR	General Data Protection Regulation, Regolamento Generale sulla Protezione dei Dati
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDP	Identity Provider
ISO/OSI	International Standards Organization Open Systems Interconnection
OTP	One Time Password
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
RSI	Responsabile della Sicurezza delle Informazioni Sielte
SMS	Short Message Service
SP	Service Provider
SP-IP	Service Provider Identità Pregresse
SPID	Sistema Pubblico di Identità Digitale
SSO	Single Sign-On

TOTP	Time Based One Time Password
UE	Unione Europea
UWP	Universal Windows Platform
NFC	Near Field Communication

- **Dati Personali**: si intende "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" (art. 4, lett. b, del Codice della Privacy - Dlgs 196/2003 ed a sensi dell'art. 4, comma 1 del Regolamento UE 2016/679 - GDPR).
- **Dati sensibili**: sono quei "dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" (art. 4, lett. d, del Codice della Privacy - Dlgs 196/2003 ed ai sensi dell'art. 9 del Regolamento UE 2016/679 - GDPR).
- **Dati giudiziari**: sono "i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale" (art. 4, lett. e, del Codice della Privacy - Dlgs 196/2003).
- **Riservatezza**: garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate.
- **Integrità**: salvaguardia dell'esattezza e della completezza dei dati e delle modalità di processo.

- **Disponibilità**: garanzia che le informazioni siano accessibili a coloro che le richiedono e ne hanno il diritto.
- **Autorizzazione**: atto che conferisce la capacità di esercitare un diritto.
- **Autenticazione**: garanzia della corretta identità dichiarata da un‘entità.

2 La tua identità digitale a portata di mano

SIELTE ID è la piattaforma realizzata da Sielte per accedere ai servizi online della Pubblica Amministrazione nel contesto del Sistema Pubblico di Identità Digitale (SPID).

SPID è il sistema di autenticazione che consente agli utenti di essere riconosciuti e di ricevere credenziali con le quali accedere a tutti i servizi pubblici e privati, il cui livello di accesso sia compatibile con quello della credenziale presentata.

Figura 1 – Logo SPID

2.1 Soggetti SPID

In SPID sono presenti i seguenti soggetti:

- **Utenti** – tutti coloro che richiedono l'Identità Digitale, i quali devono fornire alcune informazioni identificative obbligatorie, come i propri dati anagrafici e codice fiscale.
- **Identity Provider** – i soggetti che, previo accreditamento da parte di AgID e nel rispetto dei regolamenti, attribuiscono l'identità digitale ai soggetti che la richiedono, fornendo la relativa credenziale e garantendo ai service provider la verifica della credenziale medesime.

- **Attribute Provider** – i soggetti titolati che, previo accreditamento AgID e nel rispetto dei regolamenti, forniscono prova del possesso di determinati attributi e qualifiche.
- **Service Provider** – i soggetti pubblici (Agenzia delle Entrate, INPS, INAIL, ecc.) e privati che utilizzano SPID per il controllo delle credenziali di accesso ai propri servizi.
- **AgID** – svolge il ruolo di vigilanza sui soggetti accreditati ed il ruolo di garante della federazione, gestendo il registro che rappresenta l'insieme dei soggetti che hanno sottoscritto un rapporto di fiducia.

2.2 Livelli di sicurezza

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:

PRIMO LIVELLO

- corrispondente al Level of Assurance LoA2 dello standard ISO/IEC DIS 29115, dove il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a un fattore (per esempio la password), secondo quanto previsto dal presente decreto e dai regolamenti di cui all'articolo 4;

SECONDO LIVELLO

- corrispondente al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115, dove il gestore dell'identità digitale rende disponibili 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 II del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio.

TERZO LIVELLO

- corrispondente al Level of Assurance LoA4 dello standard ISO/IEC DIS 29115, dove il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato II del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio.

3 Come funziona il servizio SPID

Il sistema SPID permette ai cittadini di utilizzare un unico meccanismo di autenticazione per accedere ai servizi della pubblica amministrazione. Di seguito cerchiamo di illustrare a grandi linee il principio di funzionamento alla base del sistema SPID.

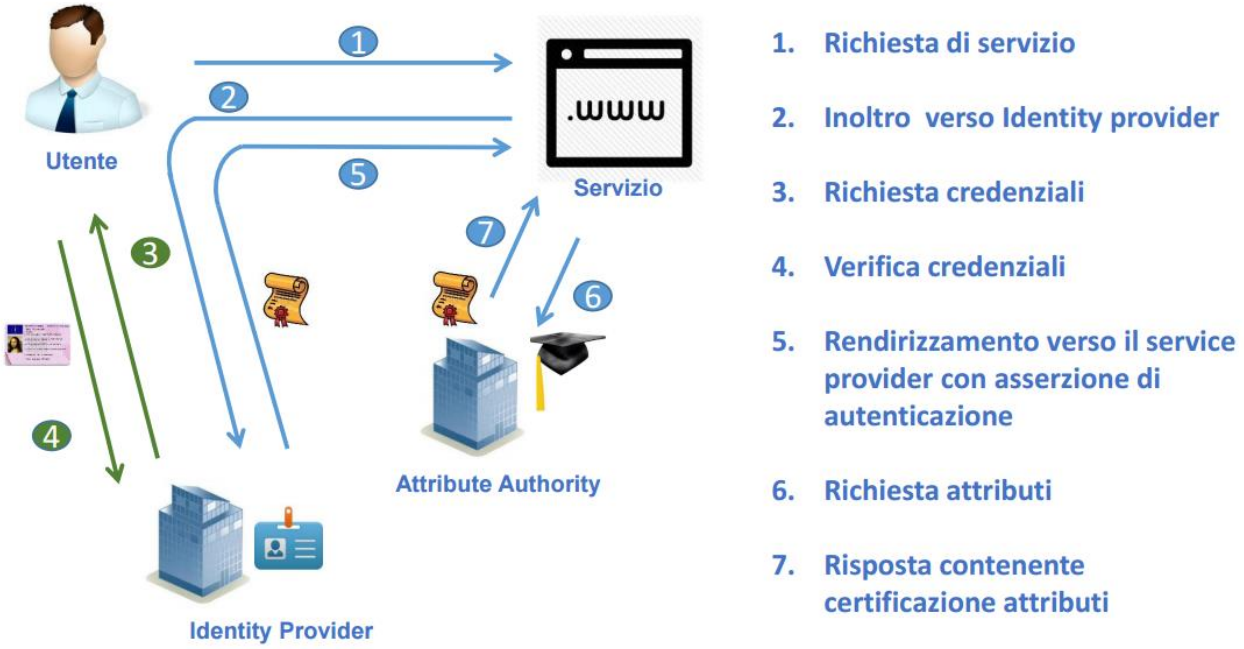


Figura 2 – Funzionamento base del sistema SPID

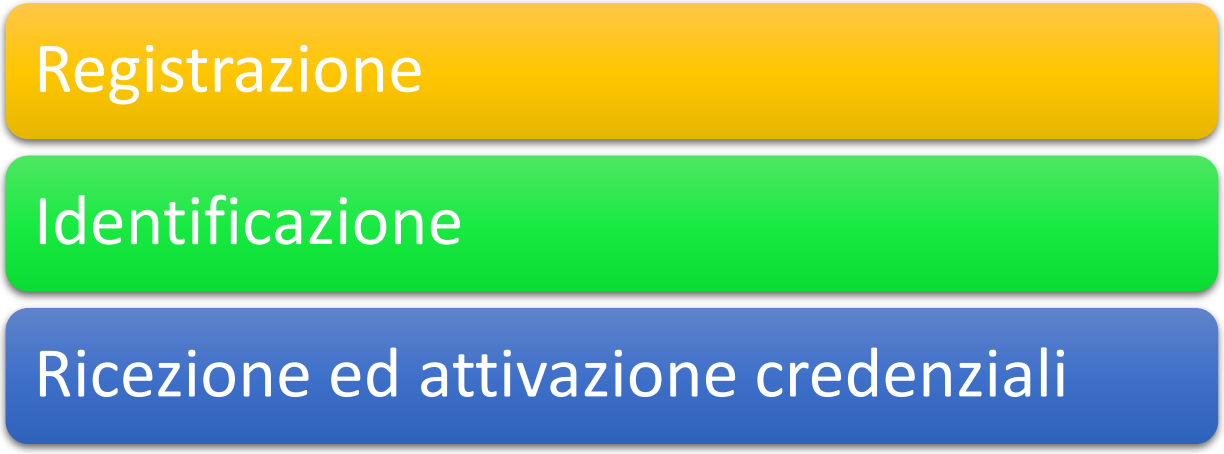
Un cittadino fa richiesta per l'identità digitale a SIELTE ID, ente accreditato presso l'AgID, e riceve le istruzioni su come utilizzare la propria identità nell'ambito della Pubblica Amministrazione.

Successivamente, se il cittadino accede ad un servizio della Pubblica Amministrazione disponibile online viene guidato nella scelta di uno degli Identity Provider accreditati e tra questi sceglie quello da cui ha ricevuto l'identità digitale. Dopo la scelta viene re-indirizzato sulla pagina web dell'Identity Provider dove inserire le credenziali per potersi autenticare. Concluso in modo positivo il processo di autenticazione, tramite un processo automatizzato, il browser

riporta il cittadino sul sito della pubblica amministrazione e, tramite meccanismi standard di interscambio di informazioni riservate, viene identificato sul sito della Pubblica Amministrazione.

4 Come ottenere l'identità digitale

Il cittadino che vuole ottenere l'identità digitale tramite SIELTE ID deve seguire la seguente procedura:



Ogni passo di questa procedura è obbligatorio per ottenere il rilascio dell'identità digitale. Di seguito viene illustrato nel dettaglio ogni singolo step da effettuare per ottenere la propria identità digitale utilizzando Sielte come Identity Provider.

4.1 Registrazione SielteID

Per richiedere l'identità digitale da utilizzare nell'ambito del servizio SPID il cittadino può connettersi al sito web https://www.sielteid.it ed effettuare la Registrazione tramite il Modulo di Adesione elettronico, oppure può recarsi presso gli uffici preposti e compilare il Modulo di Adesione Cartaceo, in presenza di un Operatore IdP Sielte.

Il Richiedente si collega al sito https://www.sielteid.it e clicca sul pulsante "Registrati".

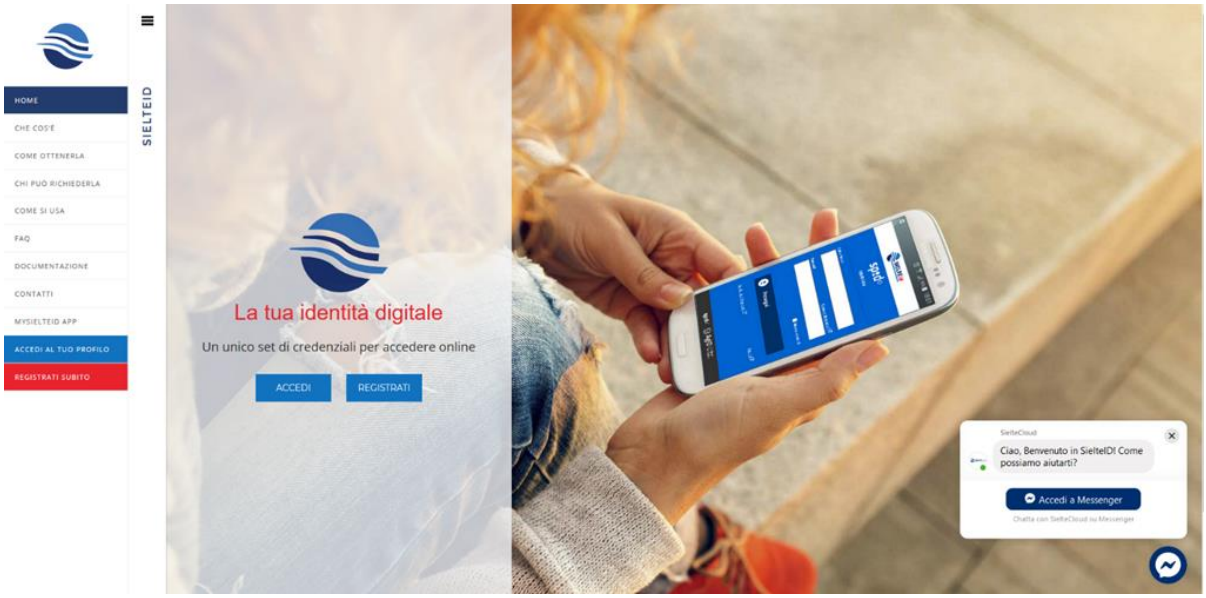


Figura 3 – Pagina SielteID

4.1.1 *Registrazione tramite sito online*

Il cittadino sceglie il tipo di profilo con cui registrarsi. In SPID vengono identificati due tipologie di utente: persona fisica (CITTADINO O LIBERO PROFESSIONISTA) e persona giuridica (AZIENDA).

Il Richiedente può selezionare la tipologia d'interesse all'inizio della fase di registrazione.

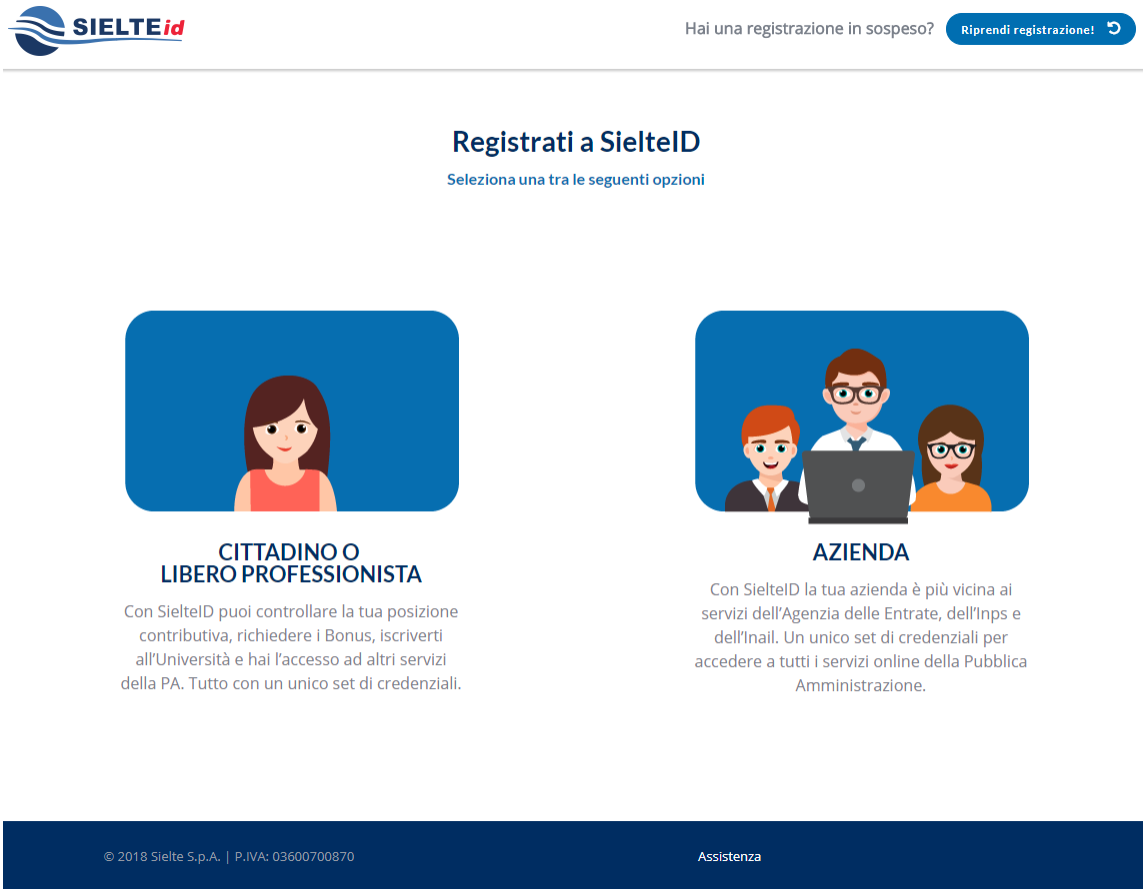


Figura 4 – Scelta della tipologia di profilo con cui registrarsi

Di seguito vengono riportati i dati obbligatori per entrambe le tipologie di utenza:

Persona Fisica

- Dati di contatto: Indirizzo mail e numero di cellulare
- Dati Personali/Anagrafici: Nome, Cognome, Codice Fiscale, Sesso, Data e Luogo di nascita, Indirizzo di Residenza
- Estremi di un valido documento di identità: Tipo, Numero, Ente di Rilascio, Data di Rilascio, Data di Scadenza

Persona Giuridica

- Denominazione/ragione sociale
- Codice fiscale o P.IVA
- Sede legale
- Visura camerale attestante lo stato di Rappresentante Legale del soggetto richiedente l'identità per conto della società (in alternativa atto notarile di procura legale)
- I Dati Personali e gli estremi del documento di identità devono essere quelli del Rappresentante Legale

Per entrambi i profili il Richiedente ha facoltà di inserire anche altre informazioni aggiuntive così come l'indirizzo PEC, che saranno associate all'identità digitale ma non utilizzate nel contesto di erogazione dei servizi da parte di Sielte.

Qualora il Richiedente debba sospendere per qualunque motivo (mancanza di rete, mancanza di disponibilità, ecc.) la fase di Registrazione, può in ogni momento riprendere da dove aveva lasciato collegandosi al sito, cliccando su "Riprendi Registrazione" ed inserendo le credenziali: username (codice fiscale/P.IVA) e password temporanea, che riceve nella e- mail di benvenuto, dopo aver compilato i suoi dati.

Durante tutta la fase di Registrazione, in alto ad ogni pagina, vengono visualizzate le attività che verranno svolte; man mano che il Richiedente prosegue con la registrazione vedrà colorarsi le icone in corrispondenza dei passaggi completati.

Il processo si compone nelle fasi descritte qui di seguito:

1. L'utente sceglie la tipologia d'interesse per cui richiede la registrazione.
2. Se ha scelto il profilo "Cittadino o Libero Professionista", il Richiedente può scegliere tra una delle sei modalità descritte di seguito, per procedere con la fase di identificazione.

   Altrimenti, se ha scelto un profilo di tipo "Azienda", la modalità di identificazione disponibile è "Firma digitale".

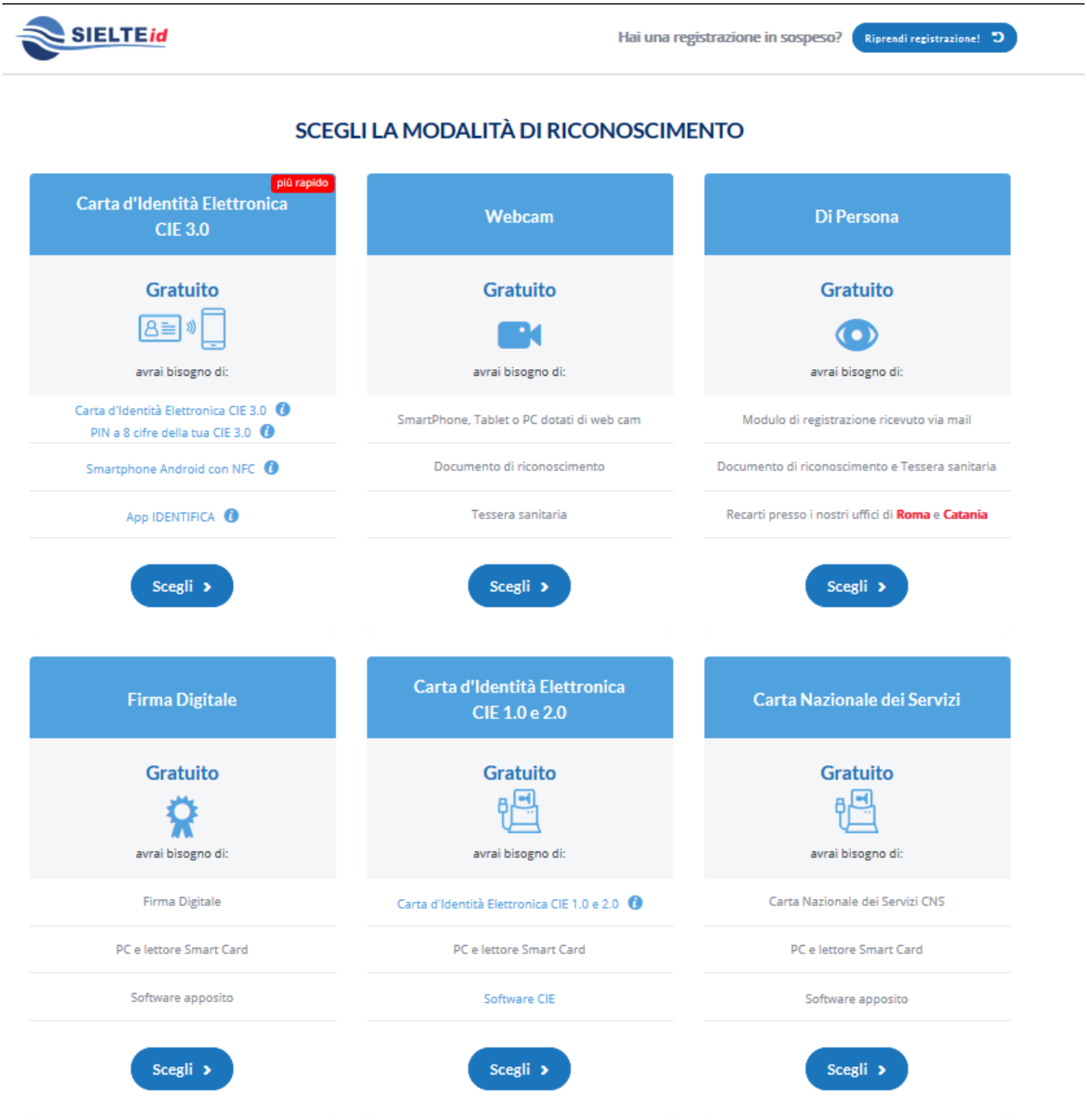


Figura 5 – Scelta della modalità di identificazione

Le modalità di identificazione vengono descritte di seguito:

a. ***Modalità Carta d'Identità Elettronica CIE 3.0:*** il Richiedente che dispone di una Carta d'Identità Elettronica CIE 3.0 e di un PIN associato alla CIE può scegliere questa modalità, identificandosi mediante l'App Sielte Identifica disponibile negli store digitali per smartphone con tecnologia NFC attiva.

b. ***Modalità Webcam***: il Richiedente viene informato che per questa modalità di identificazione deve disporre di un PC, o di uno Smartphone o di un Tablet dotati di webcam.

   Il Richiedente, prima di fissare l'appuntamento e procedere con l'identificazione tramite videochiamata da effettuare con l'Operatore IdP Sielte, troverà la data e l'ora del primo appuntamento disponibile, che potrà selezionare dopo aver inserito i dati di riconoscimento.

c. ***Modalità Di Persona***: il Richiedente per questa modalità di identificazione deve stampare e firmare il modulo ricevuto via mail durante la fase del processo di registrazione e fissare un appuntamento, scegliendo la data e la sede dove recarsi per procedere con la fase di identificazione. Riceverà, infine, il riepilogo delle informazioni via mail.

d. ***Modalità Firma Digitale:*** il Richiedente per questa modalità di identificazione deve disporre di una Smart Card e lettore. Nel caso di persona giuridica, è disponibile soltanto questa modalità di identificazione. Confermando la modalità gli vengono fornite le seguenti istruzioni: deve scaricare il Modulo di Richiesta ricevuto tramite mail, firmarlo digitalmente e caricarlo sul sistema.

e. ***Modalità Carta d'Identità Elettronica CIE 1.0 e 2.0:*** il Richiedente per questa modalità di identificazione deve disporre di una Carta d'Identità Elettronica attiva CIE 1.0 o 2.0, di un PC e di un lettore Smart Card.

f. ***Modalità Carta Nazionale dei Servizi (CNS):*** il Richiedente per questa modalità di identificazione deve disporre di una Carta Nazionale dei Servizi (CNS), di un PC e di un lettore Smart Card.

Se ha scelto la modalità Webcam, troverà una schermata in cui visualizzerà i dettagli del primo appuntamento disponibile per effettuare la videochiamata di riconoscimento.

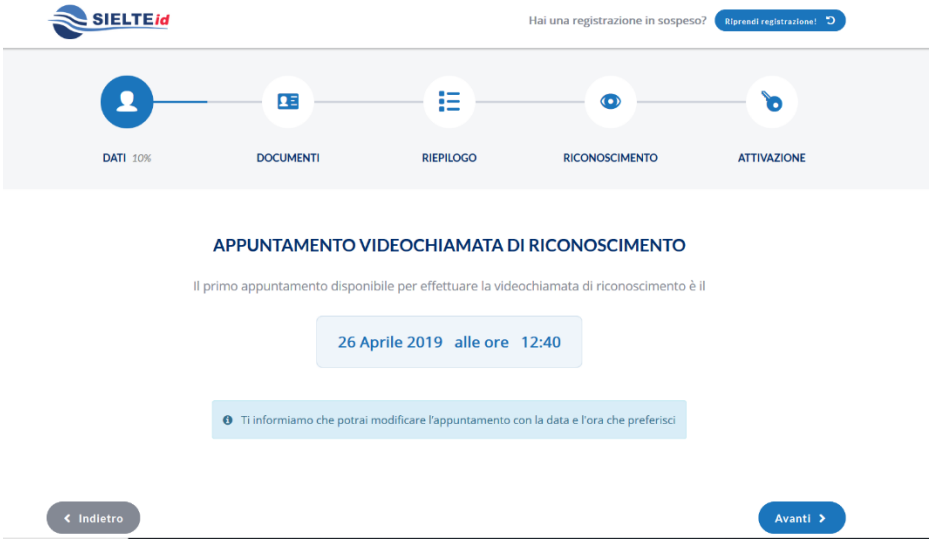


Figura 6 – Interfaccia con il primo appuntamento disponibile

3. Il Richiedente, a questo punto, sceglie se prestare il consenso all'Informativa ai sensi del D.L.vo n. 196/2003 ed ai sensi del Regolamento UE 2016/679 per il trattamento dei dati effettuato nell'ambito dei Servizi Sielte; in particolare viene informato che i dati verranno conservati, in archiviazione, per un periodo di 20 anni decorrente dalla revoca dell'identità digitale e la sessione audio/video sarà interamente conservata in modalità protetta per il periodo di 20 anni decorrente dal momento della revoca dell'identità digitale, come previsto dalla normativa vigente in materia.
4. Acconsente alla presa visione della documentazione contrattuale (Condizioni Generali Contrattuali, Manuale Operativo, Guida Utente e Guida alla sicurezza dell'identità).

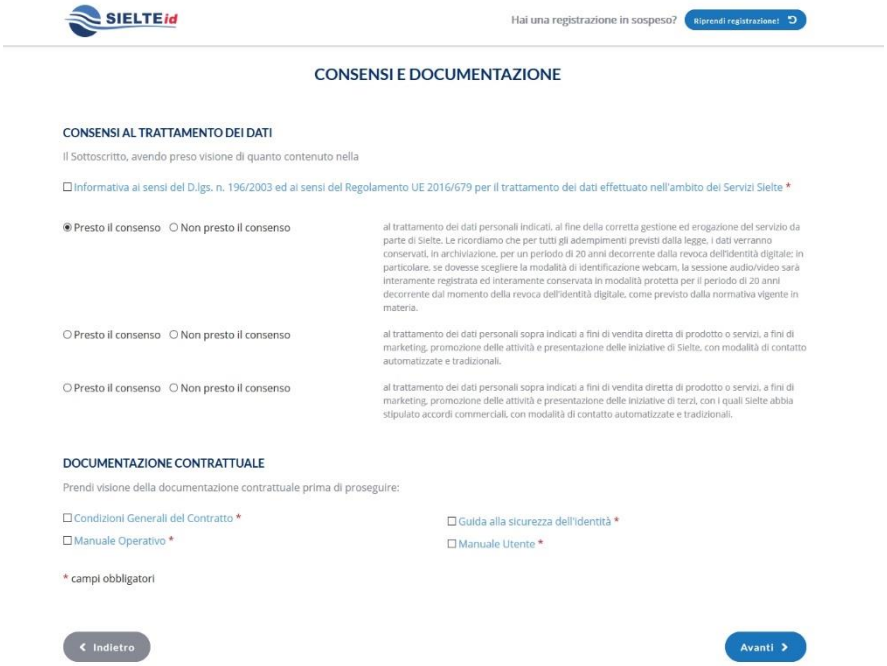


Figura 7 – Modulo di registrazione – consenso al trattamento dei dati

5. In seguito alla scelta della modalità di identificazione, il Richiedente passa alla verifica del proprio indirizzo e-mail; il sistema effettua una verifica della univocità dell'indirizzo inserito e invia un codice di verifica per verificarne la validità.

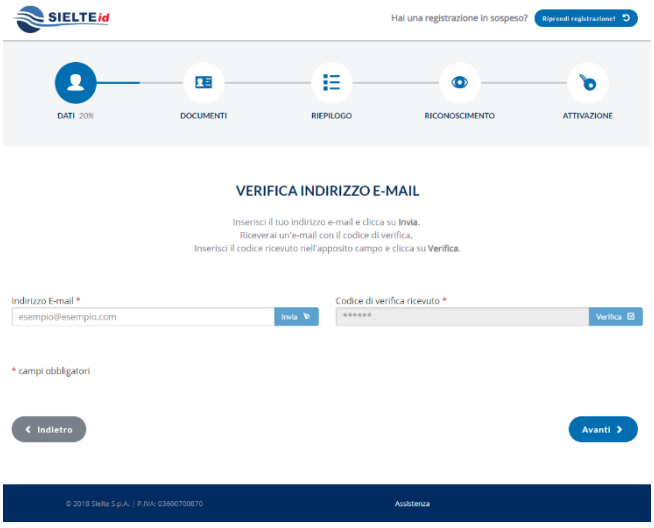


Figura 8 – Interfaccia di verifica dell'indirizzo e-mail

6. Dopo aver verificato il proprio indirizzo e-mail, inserendo il codice ricevuto via mail, il Richiedente passa all'inserimento del numero di cellulare per effettuarne la verifica e riceve un codice per verificarne la validità.

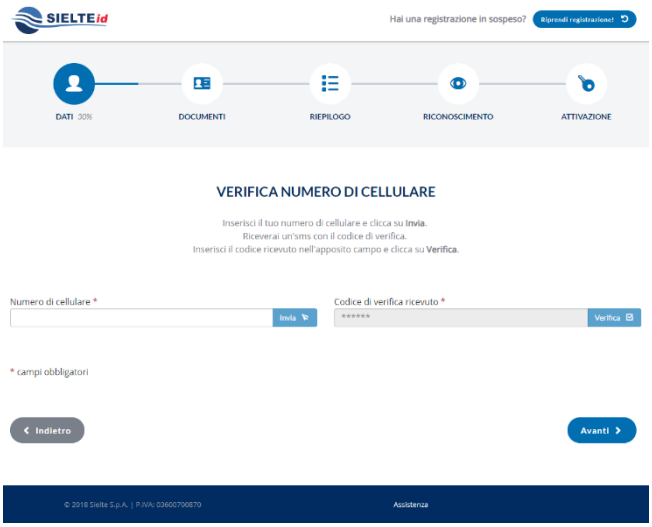


Figura 9 – Interfaccia di verifica del numero di cellulare

7. A questo punto, il Richiedente compila il modulo di richiesta elettronico, inserendo i propri dati anagrafici e i dati del domicilio. Consapevole che la falsa dichiarazione delle proprie generalità è un reato penale, per cui saranno effettuati controlli anche successivi alla fase di identificazione, dichiara sotto la propria responsabilità che le informazioni fornite corrispondono a verità.

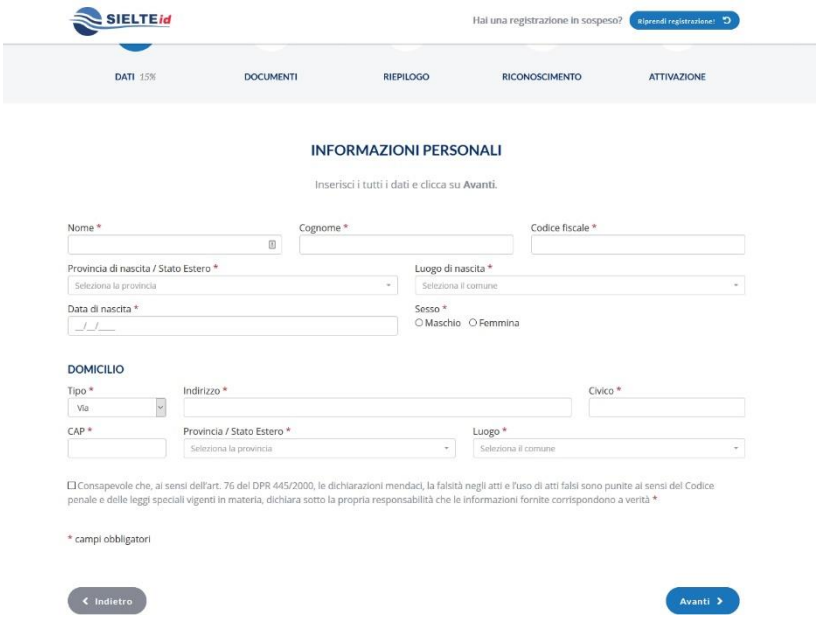


Figura 10 – Modulo di registrazione - dati personali

Nel caso di persona giuridica saranno presenti anche le sezioni riguardanti le informazioni aziendali e la sede legale.

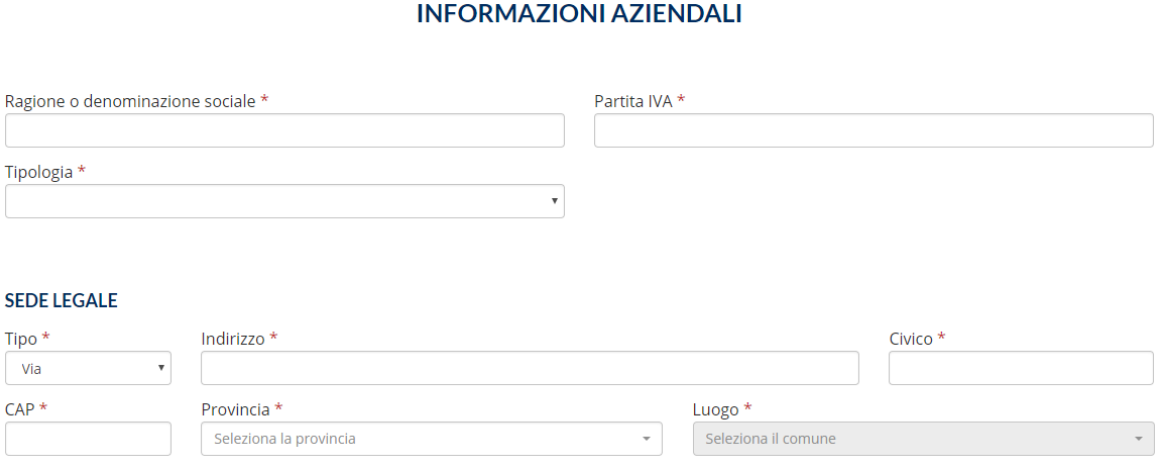


Figura 11 - Persona Giuridica: Informazioni Aziendali e Sede Legale

8. Successivamente, gli viene richiesto di inserire gli estremi del documento di identità prescelto per l'identificazione (i documenti di riconoscimento ammessi per l'identificazione sono tutti quelli ammessi dal DPR 445/2000, art. 35)[1]. Nel caso di identificazione "Webcam" o "Di Persona", il Richiedente deve allegare foto o scansione del fronte e del retro del documento di riconoscimento e della tessera sanitaria o, nel caso di soggetti sprovvisti di Tessera Sanitaria, il tesserino del codice fiscale.

Se persona giuridica, viene richiesto di caricare anche la Visura Camerale della società (o in alternativa atto notarile di procura legale), della quale ha inserito nel modulo gli estremi.

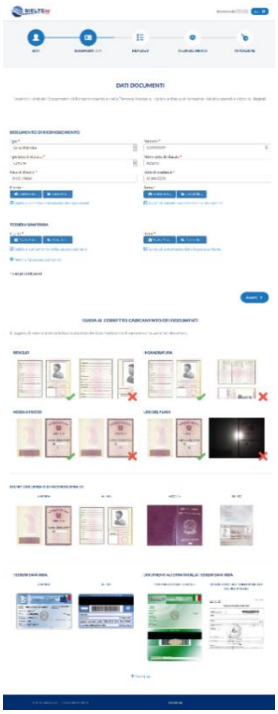


Figura 12 – Modulo di registrazione – caricamento documenti

[1] DPR 445/2000, Art. 35 Documenti di identità e di riconoscimento
1. In tutti i casi in cui nel presente testo unico viene richiesto un documento di identità, esso può sempre essere sostituito dal documento di riconoscimento equipollente ai sensi del comma 2.
2. Sono equipollenti alla carta di identità il passaporto, la patente di guida, purché' munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato.
3. Nei documenti d'identità e di riconoscimento non è necessaria l'indicazione o l'attestazione dello stato civile, salvo specifica istanza del richiedente.

9. Se il Richiedente ha scelto la modalità di identificazione **“Webcam”**, troverà in evidenza il primo appuntamento disponibile e, qualora lo desiderasse, la possibilità di poterlo modificare, decidendo la data e l’ora dell’appuntamento tra quelle disponibili e l’applicazione con cui effettuare la videochiamata. Può scegliere tra quattro opzioni: Messenger.com, Hangouts, Skype o Cisco WebEx: per le prime tre dovrà inserire un recapito (e-mail / nome utente) per essere contattato e procedere con l’identificazione. Riceverà una mail di conferma che riepiloga la data, l’ora e la tecnologia prescelta per l’appuntamento della videochiamata; nel caso in cui scelga la tecnologia Cisco WebEx all’interno della mail troverà un link per scaricare l’applicazione necessaria per la videoregistrazione.

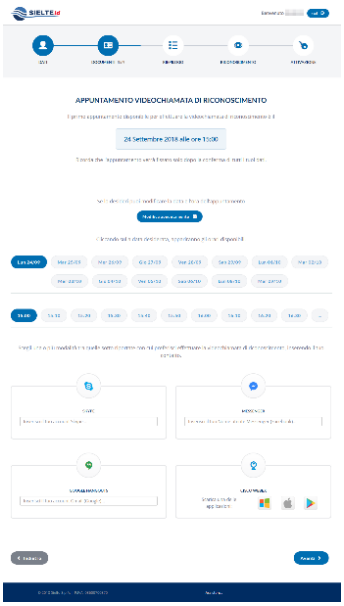


Figura 13 – Modulo di registrazione – scelta appuntamento Webcam

10. Se ha scelto la modalità di identificazione **“Di Persona”** decide la sede in cui recarsi e la data dell’appuntamento.

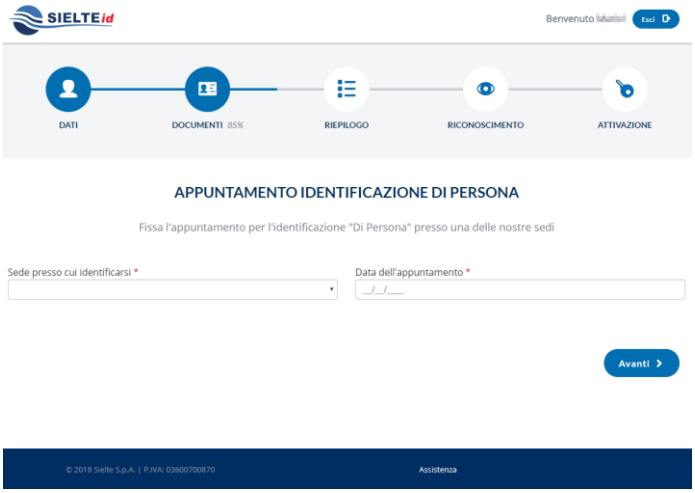


Figura 14 – Modulo di registrazione – scelta appuntamento Di Persona

11. A questo punto visualizza il Riepilogo dei dati inseriti dove può modificarli, cliccare sul pulsante “Conferma”, (vedi Figura 15 – Interfaccia riepilogo registrazione) o decidere di annullare la registrazione.

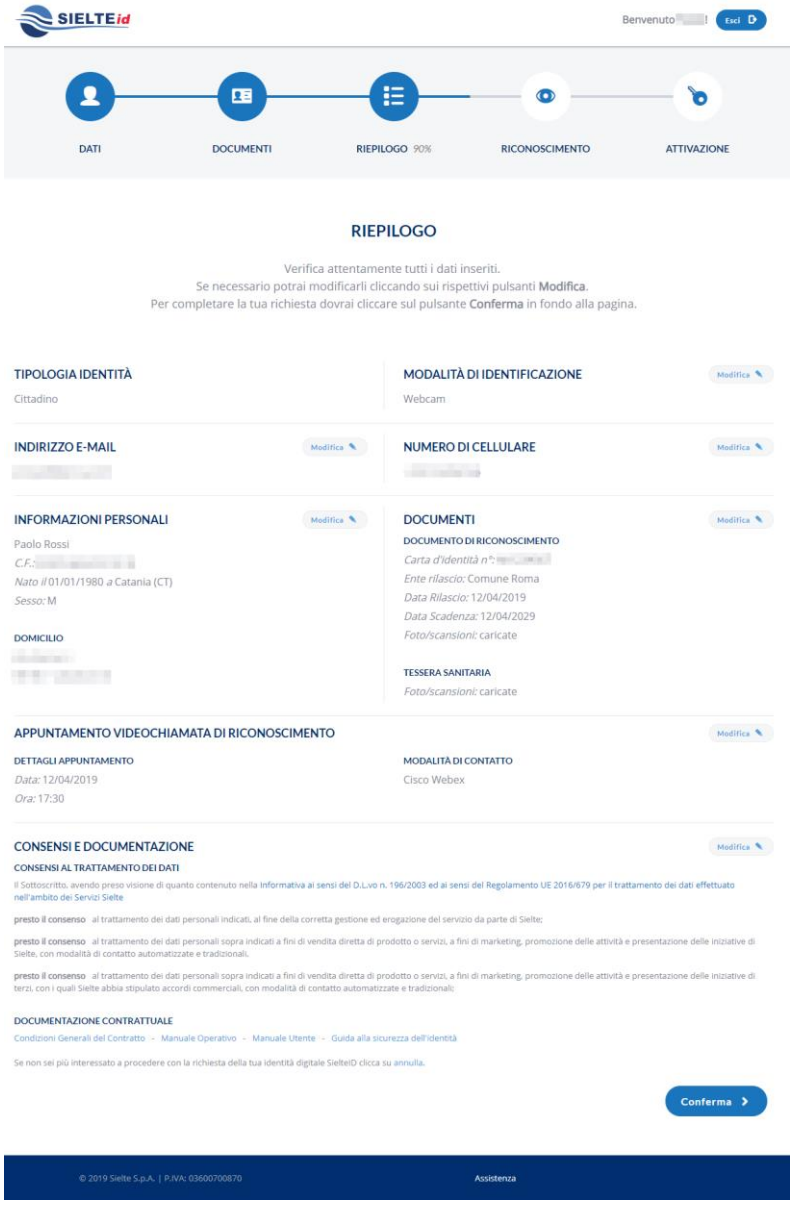


Figura 15 – Interfaccia riepilogo registrazione

12. Se possiede una **Carta di Identità Elettronica 3.0**, può identificarsi tramite l'app Identifica.

Figura 16- Identificazione CIE 3.0

Se l'utente sceglie di identificarsi con Carta d'Identità Elettronica 3.0 tramite app "Identifica", deve scaricare l'app disponibile negli store digitali per dispositivi dotati di NFC. Successivamente, all'inizializzazione dell'app, deve accedere con le credenziali temporanee ricevute nella e-mail di Benvenuto.

Figura 17 - App pagina di login

Viene richiesto di inserire il PIN di 8 cifre della carta (il PIN è composto dalla prima parte di 4 cifre ricevute nel documento Riepilogo Dati per Accettazione e dalla seconda parte di 4 cifre recapitate mezzo posta insieme alla Carta).

Figura 18- Inserimento PIN associato a CIE 3.0

Dopodiché il Richiedente deve avvicinare la carta di identità elettronica allo smartphone in prossimità del lettore NFC (alcuni dispositivi hanno il lettore sullo schermo, altri sul retro del dispositivo).

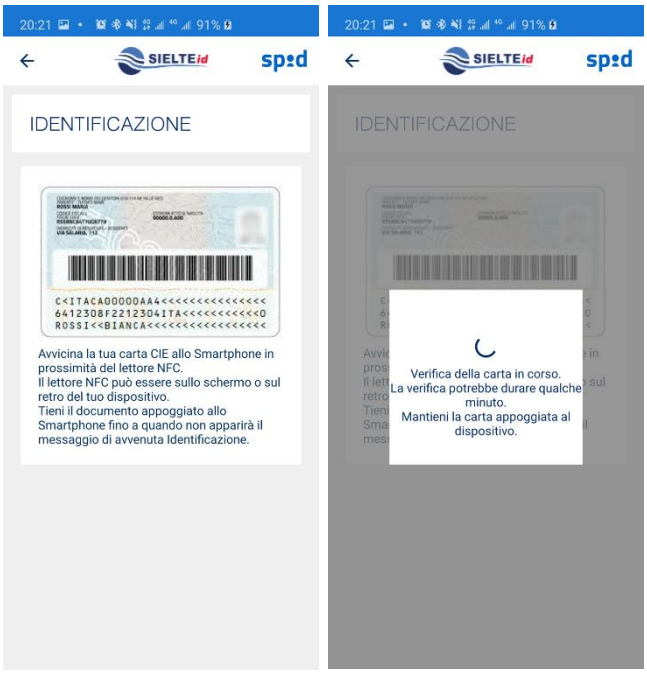


Figura 19 – Verifica della carta di identità

Se il PIN inserito è corretto e la carta viene riconosciuta, l'identificazione si conclude positivamente e l'utente riceve la mail di attivazione contenente il link per attivarsi.

13. Dopo aver confermato i dati, se ha scelto la modalità **"Firma digitale"**, l'utente firma digitalmente con un software di firma digitale il Modulo di adesione e lo carica sul sistema. L'Operatore Sielte IdP effettuerà la verifica sulla validità della firma digitale apposta sul documento; in caso di verifica positiva, l'utente riceve la mail di conferma di avvenuta identificazione e può procedere all'attivazione della sua identità digitale.

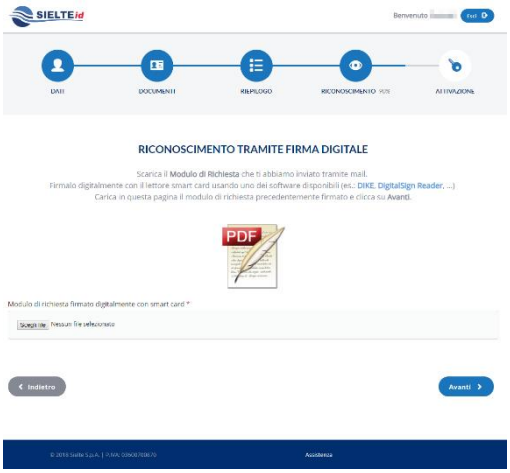


Figura 20 – Modulo di registrazione – identificazione firma digitale

Il sistema informa il Richiedente che il documento è stato caricato con successo e di attendere una mail di conferma circa l'avvenuta identificazione (che riceverà dopo la verifica del documento da parte di un Operatore IdP).

14. Se l'utente sceglie l'identificazione con CIE 1.0, 2.0 o CNS tramite smartcard, deve inserire la carta all'interno del lettore e collegarlo in pc, come in figura 21, ed inserire il PIN richiesto. Se il PIN è corretto, il Richiedente viene identificato.

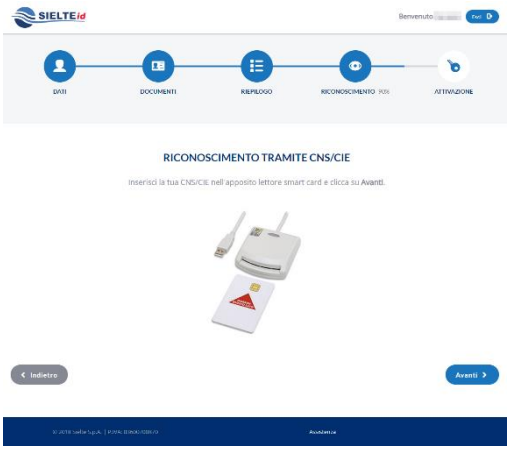


Figura 21– Modulo di registrazione – identificazione CIE/CNS

4.1.1.1 REGISTRAZIONE IDENTITÀ PREGRESSA CON MIGRAZIONE ASSISTITA

Il Richiedente ha la possibilità di ottenere la sua identità digitale tramite l'SP-Ip presso cui ha un account; il profilo viene trasferito presso l'Identity Provider scelto dal titolare, in cui dovrà completare la registrazione.

Lo scenario prevede che l'utente, obbligatoriamente autenticato, possa essere reindirizzato su sua richiesta verso un IdP, in cui troverà la maschera di registrazione precompilata con i dati forniti obbligatoriamente dall'SP-Ip: Nome, Cognome e Codice Fiscale.

L'utente può effettuare la procedura di richiesta dell'Identità Digitale completando la registrazione secondo quanto descritto nel paragrafo 4.1 e la fase di identificazione secondo quanto descritto nel paragrafo 4.2

4.1.1.2 REGISTRAZIONE IDENTITÀ PREGRESSA

Il Richiedente ha la possibilità di ottenere la sua Identità Digitale tramite l'SP presso cui ha un'identità; il profilo viene trasferito presso l'IdP scelto dal titolare che dovrà completare la registrazione con le altre informazioni necessarie per ottenere l'Identità Digitale SPID. L'utente, dopo aver effettuato l'autenticazione sul servizio dell' SP, con un livello SPID 2 (LoA3), clicca sul pulsante "Ottieni SPID"; a quel punto l'SP trasmette i dati obbligatori all'IdP scelto dall'utente, cioè Nome, Cognome e Codice Fiscale, e completa la registrazione secondo quanto descritto nel paragrafo 4.1 dal punto 3 in poi, con le sole differenza che non occorrerà caricare i documenti come in Figura 12 e che dopo il riepilogo l'utente verrà identificato automaticamente.

Una volta attivato, sarà compito dell'IdP comunicare all'SP da cui proviene l'utente l'avvenuta attivazione.

4.1.2 *Registrazione negli uffici preposti*

Il Richiedente ha la possibilità di ottenere la sua identità digitale attraverso la compilazione del Modulo di adesione in forma cartacea, optando per la Registrazione ed Identificazione a vista tramite modulo cartaceo.

Il Richiedente si reca in uno degli uffici Sielte preposti, consultabili tramite la mappa all'interno del sito www.sielteid.it, o presso gli Uffici di Registrazione Autorizzati, compila il Modulo di Adesione, prende visione e presta il consenso, qualora necessario, dell'Informativa al trattamento dei dati ed alle Condizioni Generali del Servizio; infine firma il Modulo.

Il Richiedente deve esibire all'Operatore IdP preposto il documento di riconoscimento, i cui estremi sono stati inseriti all'interno del modulo, integro, con fotografia e firma autografa ed in corso di validità e la tessera sanitaria attestante il codice fiscale o, nel caso di soggetti sprovvisti di Tessera Sanitaria, il tesserino del codice fiscale.

L'Operatore IdP ne verifica l'idoneità e ne acquisisce copia. Il Richiedente completerà la sua fase di identificazione solo dopo un'ulteriore fase di verifica dei documenti già effettuata dall'Operatore IdP, dopo aver validato il proprio indirizzo mail e numero di telefono.

4.2 Identificazione SielteID

Ogni richiesta assegnata all'Operatore IdP viene gestita dallo stesso, effettuando le verifiche necessarie a validare i documenti e verificando la stessa identità del Richiedente attraverso l'accesso alle fonti autoritative.

Inoltre, l'Operatore IdP verifica che il documento di riconoscimento caricato per le modalità di identificazione "Webcam" o "Di Persona" sia integro ed in corso di validità, rilasciato da un'Amministrazione dello Stato, munito di fotografia e firma autografa dello stesso e controlla la validità della tessera sanitaria attestante il codice fiscale o, nel caso di soggetti sprovvisti di Tessera Sanitaria, il tesserino del codice fiscale.

Sielte è responsabile della valutazione in merito alla veridicità delle informazioni relative all'identità, quindi l'operatore preposto all'attività, in caso di verifiche negative o per mancanza parziale o totale della documentazione richiesta, non avvia la fase di identificazione e quindi di attivazione dell'ID, bensì contatta il Richiedente tramite mail chiedendo di caricare la documentazione valida in sostituzione a quella presentata, piuttosto che caricare quella mancante.

La fase di identificazione si differenzia in base alla Modalità prescelta in fase di Registrazione dal Richiedente, come già descritto all'interno del paragrafo 4.1 Registrazione SielteID.

4.3 Ricezione ed Attivazione credenziali SPID

La consegna dell'identità digitale e delle credenziali al cittadino che ne ha fatto richiesta e che è stato identificato, viene eseguita per via telematica tramite processo innescato dal Gestore di Identità Sielte. Nella fase di rilascio dell'identità digitale l'utente riceve, all'indirizzo mail inserito in fase di registrazione, le seguenti informazioni:

- **Codici dispositivi** – i codici dispositivi sono il codice di sospensione, il codice di sblocco ed il codice di revoca, utili per la gestione dell'identità digitale e delle credenziali nel loro intero ciclo di vita.
- **Link di attivazione** – è il link su cui l'utente deve cliccare, o se preferisce copiare e incollare nel browser, per procedere con l'attivazione del suo profilo.

Quindi, l'Utente attiva la propria identità digitale cliccando sul link "Attiva il tuo profilo", inserisce all'interno della schermata che visualizza, nel campo "Vecchia password", la Password temporanea ricevuta all'interno della "Mail di Benvenuto" in fase di Registrazione e la modifica inserendone una nuova, rispettando i criteri di sicurezza descritti a fianco, e infine sceglie la domanda segreta.

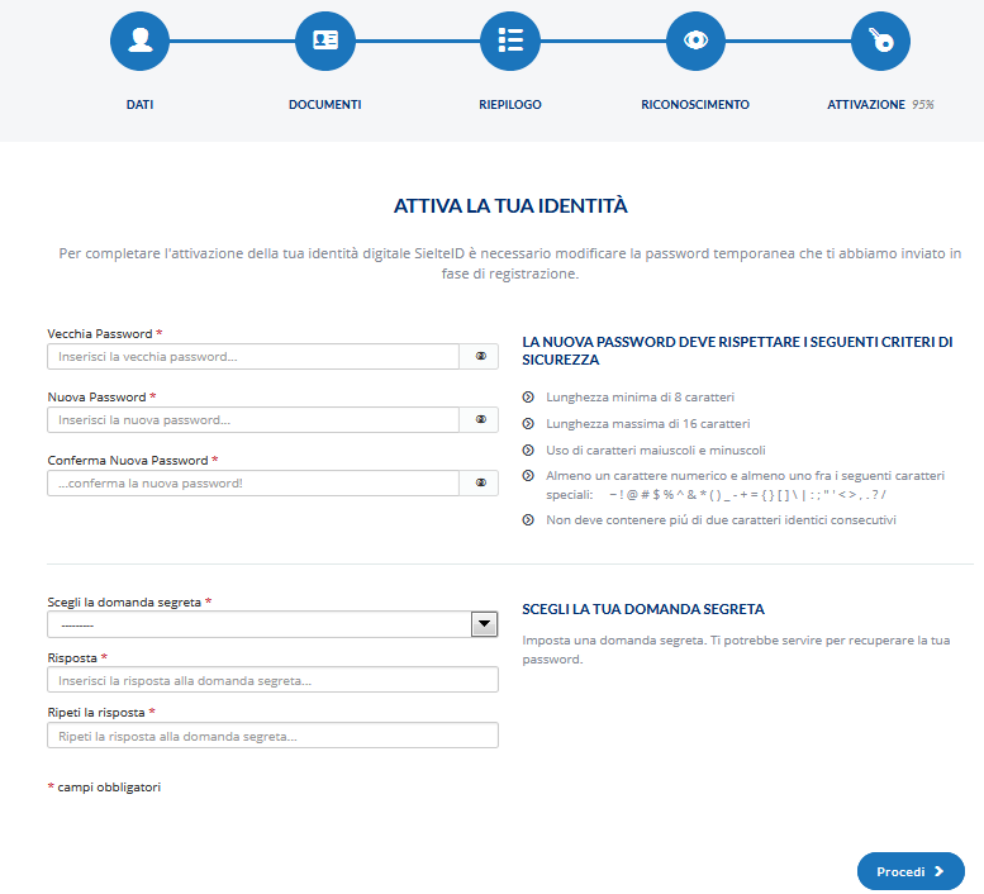


Figura 22-Interfaccia di attivazione identità

L'Identità adesso è attiva e l'Utente ha attive le credenziali di Livello 1 SPID.

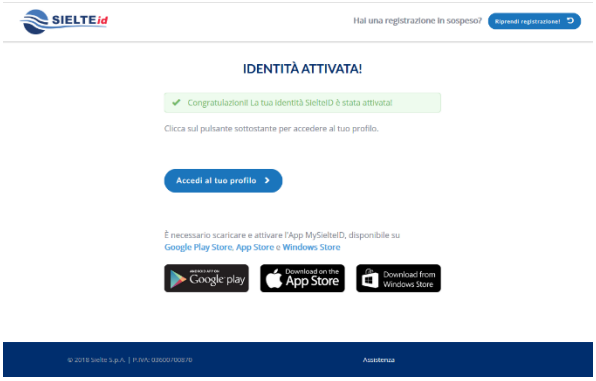


Figura 23-Interfaccia di conferma identità attivata

Per accedere a determinati servizi della Pubblica Amministrazione ed operazioni del proprio profilo, l'utente dovrà attivare le credenziali di livello 2. Per l'attivazione di tali credenziali, dovrà associare un dispositivo smartphone tablet, o desktop (nel solo caso Windows), alla sua identità digitale (vedi paragrafo 7.3.3), installando l'app MySielteID (vedi paragrafo 7.3.1) disponibile su App Store, Google Play Store e Windows Store.

5 Utilizzo dell'identità digitale

L'utente, tramite la propria identità digitale, può accedere online ai diversi servizi della Pubblica Amministrazione, scegliendo l'Identity Provider SielteID ed immettendo le proprie credenziali SPID (come in Figura 24- Esempio di utilizzo accesso SielteID.).

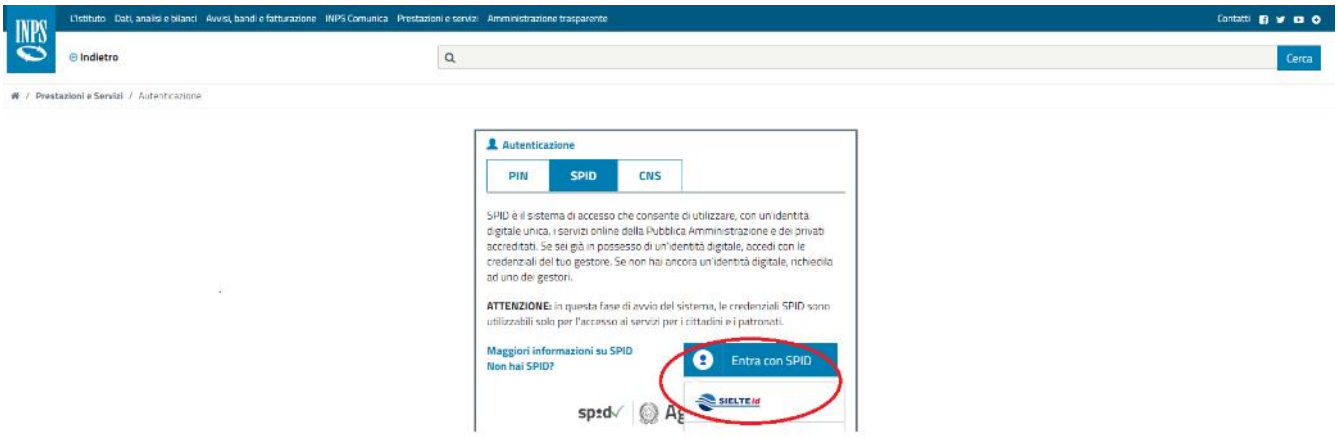


Figura 24- Esempio di utilizzo accesso SielteID

Sielte mette a disposizione dell'utente tre livelli di funzionalità per l'autenticazione dell'identità digitale:

- Autenticazione di Livello 1 SPID
- Autenticazione di Livello 2 SPID
- Autenticazione di Livello 3 SPID

Il Livello di sicurezza 1 SPID permette all'utente l'autenticazione ad un fattore tramite l'utilizzo della coppia UserID e Password.

Il livello di sicurezza per questo tipo di autenticazione si basa sulla complessità della password. Le policy definite dall'Identity Provider sono conformi a quanto stabilito dall'AgID per il sistema SPID.

Se l'utente inserisce più volte la password errata, il sistema prevede il blocco temporaneo delle credenziali.

Il Livello di sicurezza 2 SPID permette all'utente l'autenticazione a due fattori, tramite l'utilizzo della coppia UserID e Password e di un codice OTP generato tramite l'app MySielteID.

La consegna delle credenziali può avvenire nelle seguenti modalità:

- Credenziali con sicurezza di Livello 1 SPID – in questo caso viene creata una password temporanea, che viene inviata all'utente via posta elettronica, durante la fase di registrazione nella mail di Benvenuto. Successivamente, l'utente dovrà necessariamente impostare una nuova password con i seguenti criteri di protezione: lunghezza di 10 caratteri che contiene caratteri maiuscoli e minuscoli, contiene almeno un carattere numerico, non contiene più di due caratteri identici consecutivi e contiene almeno un carattere speciale (#, $, %, ecc.). Effettuato il cambio della password, l'utente può impostare la domanda segreta e quindi visualizzare i propri dati.
- Credenziali con sicurezza di Livello 2 SPID – in questo caso viene utilizzato lo stesso meccanismo per il rilascio delle credenziali di Livello 1 SPID. In aggiunta, in fase di autenticazione, viene utilizzato un codice numerico temporaneo OTP (della durata di 60 secondi) da utilizzare in accoppiata alle credenziali di Livello 1; il codice è disponibile tramite l'app MySielteID.

Il Livello di sicurezza 3 SPID permette all'utente l'autenticazione a due fattori, tramite l'utilizzo della coppia (UserID, Password) e di un dispositivo smartcard con all'interno il certificato di autenticazione contenuto nelle CIE/CNS e TS-CNS in corso di validità.

L'operazione per attivare le credenziali di Livello 3 è disponibile dalla pagina del proprio profilo SielteID, su "Gestione Servizi" nella sezione Spid Liv3, oppure nella sezione "Aggiungi Credenziale" (vedi par.7.2.3).

6 Come gestire l'identità digitale

Sielte mette a disposizione dell'utente un'interfaccia web, alla quale l'utente può accedere tramite le credenziali SPID e grazie alla quale può gestire le informazioni relative al proprio profilo e può usufruire delle funzioni che garantiscono il corretto ciclo di vita dell'identità digitale e delle credenziali associate ad essa.

La gestione del ciclo di vita dell'identità digitale si articola nei processi illustrati in Figura 25- Ciclo di vita dell'identità digitale:

Figura 25- Ciclo di vita dell'identità digitale

Successivamente vengono descritte le funzionalità del proprio profilo utente.

7 Interfaccia utente

Gli utenti che hanno ottenuto la propria identità digitale tramite il servizio SIELTE ID hanno a disposizione un'area riservata, accessibile tramite il sito web https://www.sielteid.it cliccando su "Accedi", oppure su "Accedi al tuo profilo".

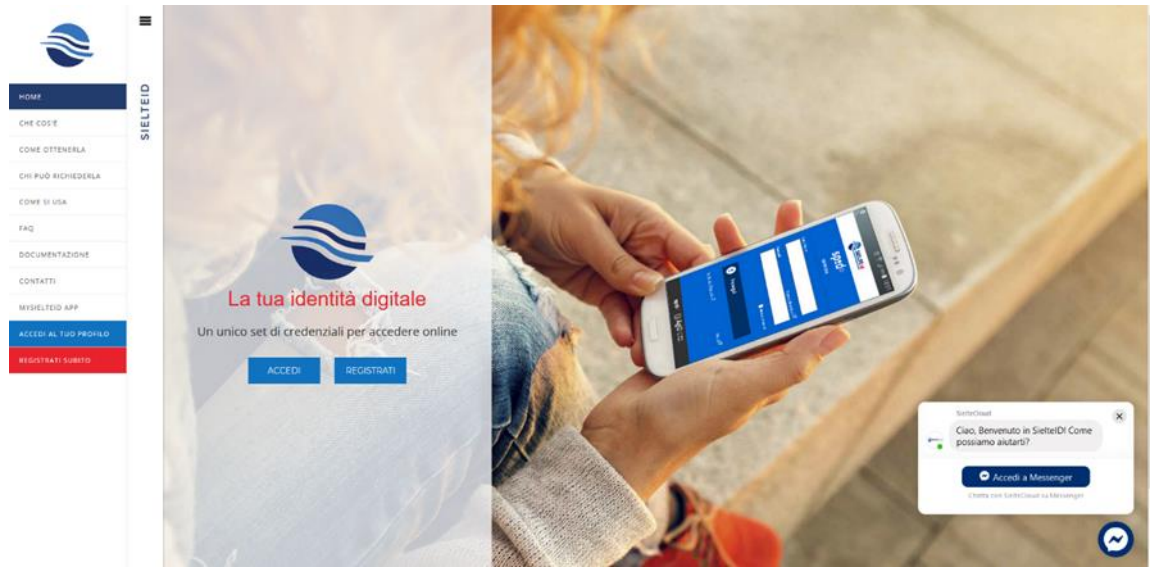


Figura 26 – Pagina SielteID

Autenticandosi con le proprie credenziali SPID, cioè Codice Fiscale e Password, l'utente ha accesso al proprio profilo SielteID.

Figura 27 – Login di SielteID

Nel caso in cui venga dimenticata la propria Password, cliccando sulla funzione “Recupero Password” (vedi Figura 27 – Login di SielteID) è possibile richiedere una nuova password, come successivamente spiegato al capitolo 9.

Una volta effettuato correttamente l’accesso alla pagina del proprio profilo SielteID, l’utente può visualizzare i servizi abilitati a SPID (vedi paragrafo 7.1); nella pagina in alto a destra, l’utente visualizza lo stato dell’identità SPID, tramite l’etichetta Attivo, e ha la possibilità di effettuare il logout, tramite la voce “Esci”, come mostrato in Figura 28 – Interfaccia iniziale del profilo SielteID all’avvenuto accesso).

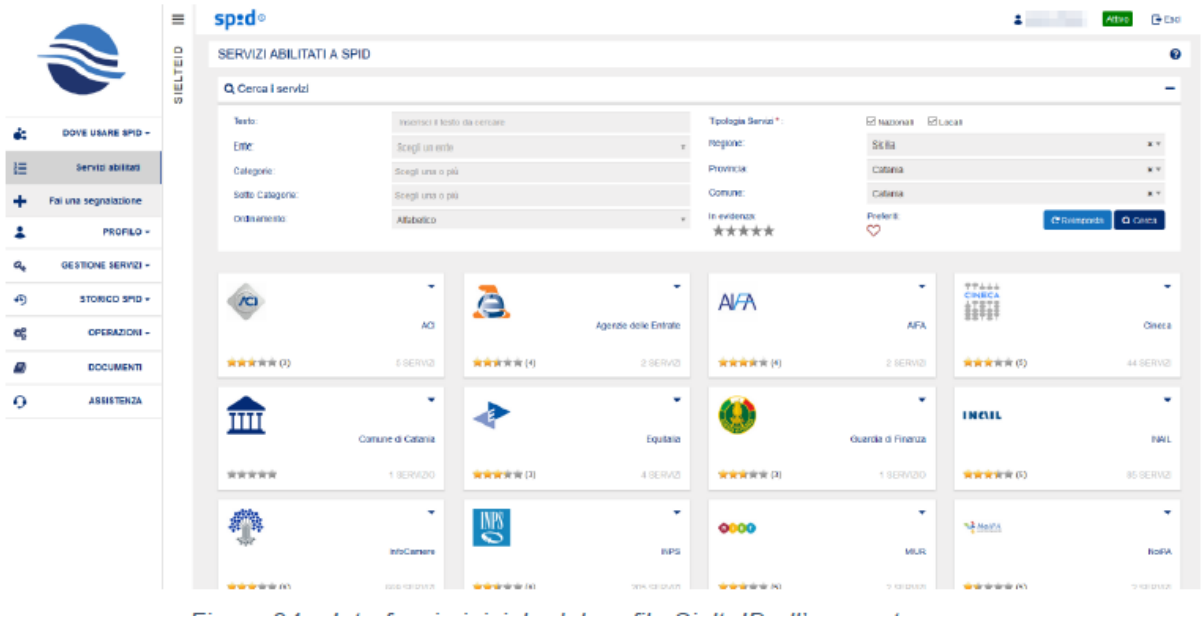


Figura 28 – Interfaccia iniziale del profilo SielteID all'avvenuto accesso

L'utente può gestire il proprio account ed effettuare (sotto la voce "Operazioni", vedi paragrafo 7.5) cambio password, cambio numero di cellulare, cambio dell'indirizzo mail, aggiornare il proprio documento, sospendere la propria identità digitale o revocarla.

Tali operazioni, però, richiedono un accesso di livello 2, come spiegato nel capitolo 8.

7.1 Servizi abilitati a SPID

Grazie al servizio "Dove usare SPID", fornito al cittadino, Sielte mette a disposizione una comoda interfaccia interattiva, utile per agevolare l'utente che ha un profilo SielteID, a ricercare i servizi di cui può disporre con la propria identità digitale.

L'utente può visualizzare i servizi più utilizzati, sceglierli, applicando determinati filtri, e memorizzarli tra i propri preferiti fra quelli che predilige maggiormente (paragrafo 7.1.1).

Inoltre, può segnalare un nuovo servizio, non ancora presente nel catalogo, un servizio non funzionante o dismesso, che sarà prontamente elaborato dal supporto (paragrafo 7.1.2).

7.1.1 *Servizi abilitati*

All'accesso, l'utente troverà i servizi abilitati a SPID all'interno della sezione "Dove usare SPID". In quest'area il cittadino può visualizzare la lista dei servizi abilitati su SPID.

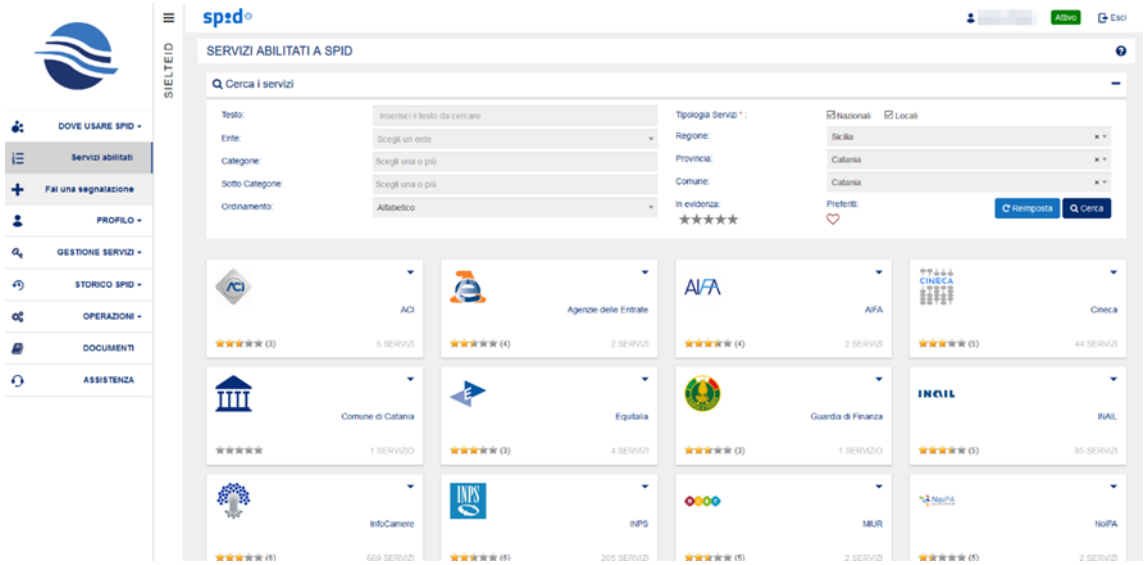


Figura 29 – Interfaccia del catalogo dei servizi abilitati a SPID

Nel riquadro "Servizi abilitati a SPID" è possibile visualizzare l'elenco degli enti pubblici e, cliccando su ciascuno di essi, accedere alla lista dei servizi associati per quel determinato ente.

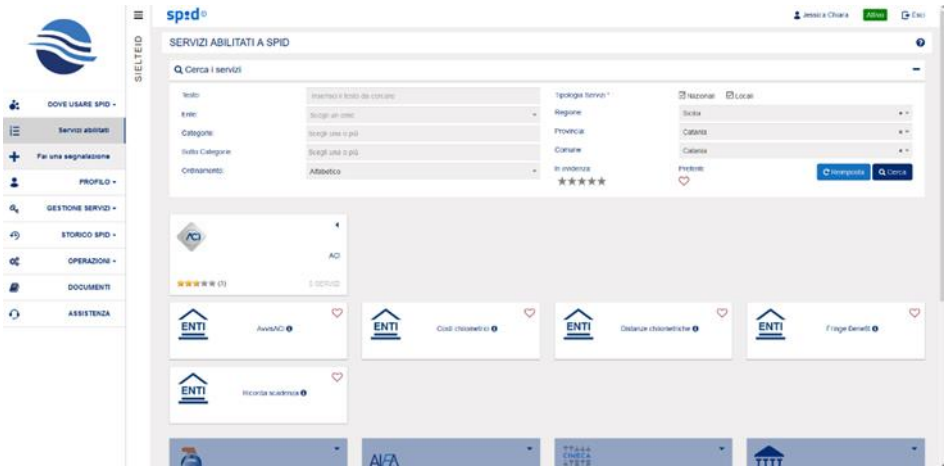


Figura 30 – Lista dei servizi abilitati a SPID

L'utente può valutare un determinato ente, cliccando sull'icona all'intero del riquadro. Un maggior numero di stelle indica un maggiore livello di gradimento; nessuna stellina indica che non è stata effettuata alcuna valutazione e, quindi, non un basso livello di gradimento.

L'icona badge +3 NEW , all'interno del riquadro di un ente, indica il numero di nuovi servizi che sono stati associati per quel determinato ente.

L'utente può inserire un servizio nella lista dei suoi preferiti, cliccando sull'icona all'interno del riquadro; troverà tali servizi preferiti scelti anche nell'app MySielteID, vedi paragrafo 7.3.1.

Cliccando sulla barra di ricerca in alto, compare un riquadro, in cui l'utente può ricercare un servizio, filtrandolo mediante: un testo libero, il nome dell'ente, una determinata categoria o sottocategoria, tipologia di servizi (nazionali o locali), regione, provincia, comune, indice di evidenza (scelto in base al numero di stellette), filtrarlo tra i propri preferiti e scegliere di ordinare gli enti secondo ordine alfabetico o di valutazione.

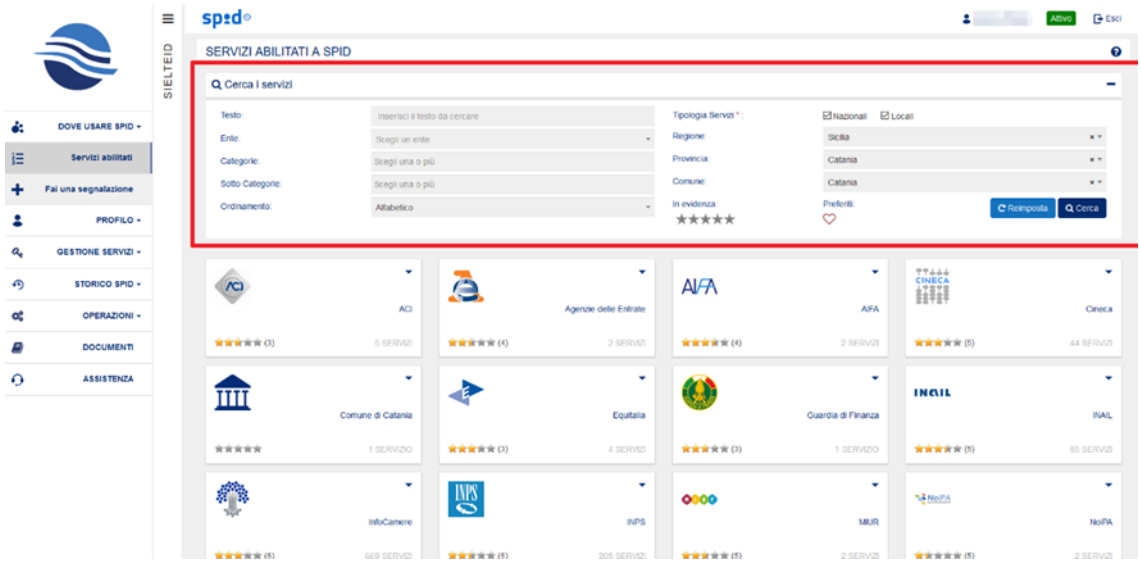


Figura 31 – Riquadro di ricerca dei servizi

7.1.2 *Fai una segnalazione*

All'interno della sezione "Fai una segnalazione", il cittadino può segnalare un nuovo servizio non ancora presente nel catalogo, un servizio non funzionante o dismesso.

Al fine di rendere più efficace la segnalazione, l'utente è invitato ad essere il più dettagliato possibile, riportando, preferibilmente, il riferimento all'ente o al servizio da aggiungere.

Inoltre, viene richiesto che il testo del messaggio abbia una lunghezza minima di 30 caratteri.

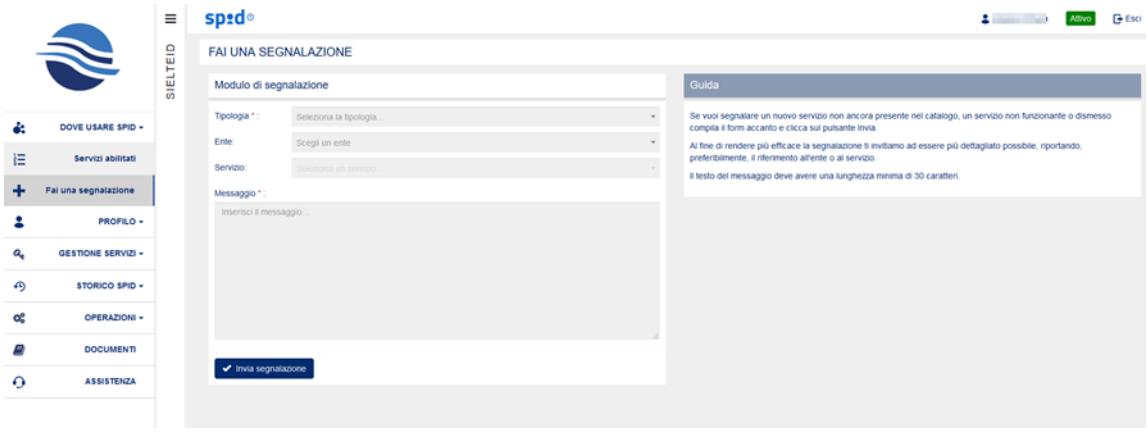


Figura 32 – Riquadro per effettuare una segnalazione

7.2 Profilo

7.2.1 *Il tuo profilo*

Nella sezione “Il tuo profilo”, all’interno di “Profilo”, è possibile visualizzare le informazioni personali inserite in fase di registrazione dall’utente, gli attributi identificativi e non identificativi.

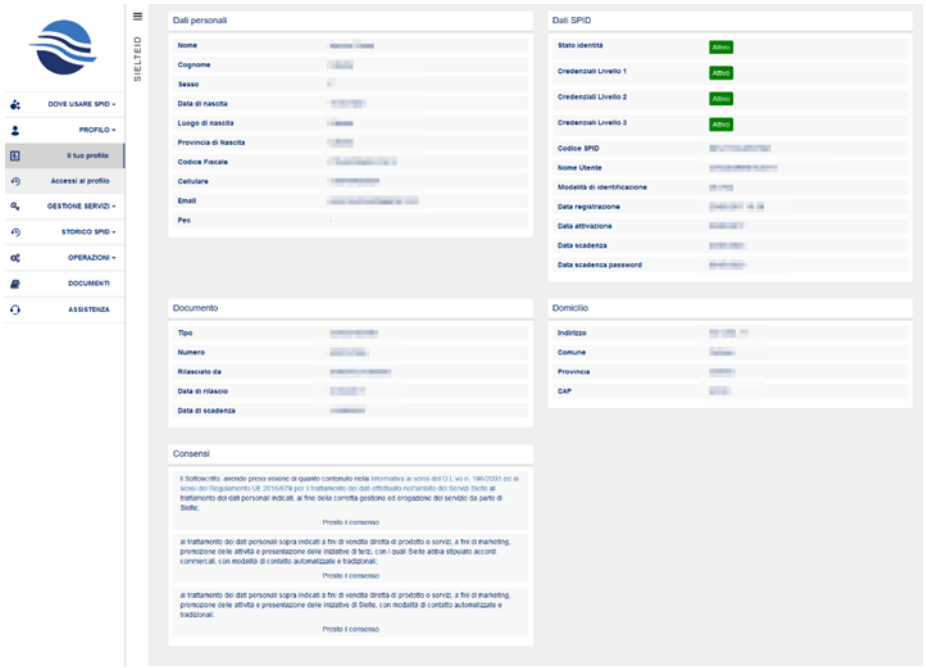


Figura 33 – Interfaccia dei dati personali del profilo SielteID

All’interno del riquadro “Dati Personali” sono visibili le informazioni personali dell’utente.

All’interno del riquadro “Dati SPID” l’utente può visualizzare lo stato della propria identità, lo stato di attivazione delle credenziali, il proprio codice identificativo SPID, il proprio nome utente, la modalità di identificazione scelta ed effettuata, la data di registrazione, la data di attivazione e la data di scadenza delle credenziali.

All’interno del riquadro “Documento” è descritto il tipo di documento caricato ed il suo numero identificativo, il comune che lo ha rilasciato e le relative date di rilascio e scadenza.

All'interno del riquadro "Domicilio" sono presenti i dati domiciliari relativi al cittadino, inseriti in fase di registrazione, tra i quali: indirizzo, comune di residenza, provincia e CAP.

Nel caso di persona giuridica saranno visibili le sezioni aggiuntive: "Dati azienda" e "Sede legale".

Infine, tramite il pulsante Modifica, in alto a destra, è possibile modificare i dati relativi al "Domicilio" e i "Consensi al trattamento dei dati personali". Questa operazione richiede un'autenticazione di livello 2 (vedi capitolo 8).

7.2.2 *Accessi al profilo*

Cliccando su "Accessi al profilo", all'interno della voce "Profilo", l'utente può visualizzare in forma tabellare l'elenco di tutti gli accessi effettuati al profilo SielteID, filtrandoli tramite opportune opzioni tra le quali ad esempio, l'intervallo di tempo desiderato e il livello di accesso (se di tipo 1 o 2).

Questa operazione richiede un'autenticazione di livello 2, vedi capitolo 8.

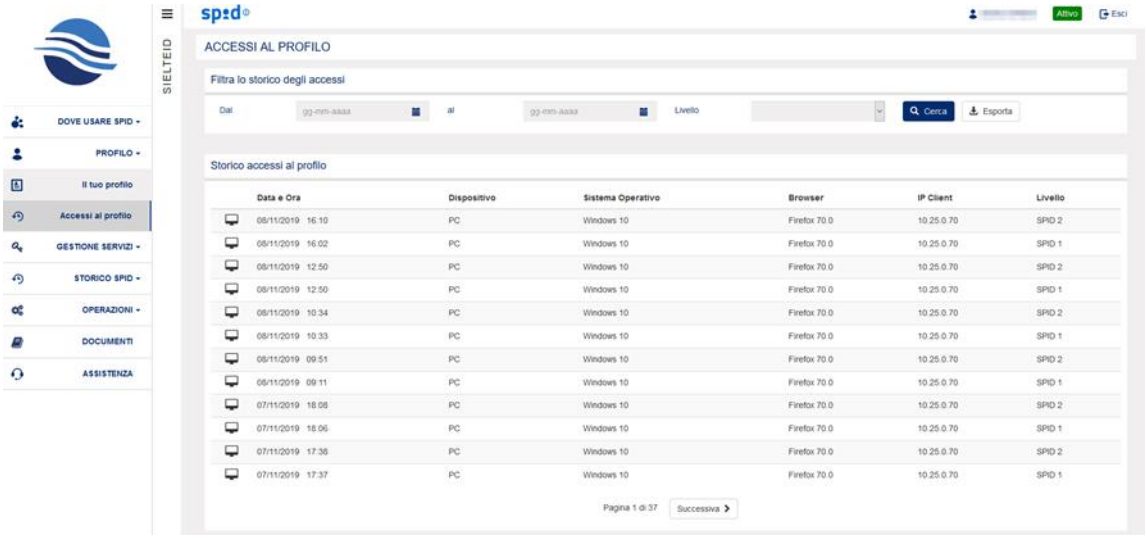


Figura 34 – Interfaccia dello storico accessi al profilo

Nell'elenco presente in Figura 34 sono riportate le informazioni riguardanti la data e l'ora di accesso, il dispositivo utilizzato, il sistema operativo, il browser, l'indirizzo IP del dispositivo dell'utente ed il livello di sicurezza. L'utente, inoltre, tramite il tasto "Esporta", può memorizzare tali informazioni, esportandole in un file .xls.

7.3 Gestione servizi

Nella sezione "Gestione Servizi" è possibile aggiungere i Servizi SPID Livello 2 e Livello 3.

Di seguito illustriamo come:

7.3.1 *App MySielteID- Spid LIV 2*

Sielte mette a disposizione degli utenti che hanno ottenuto la propria identità digitale con SielteID l'applicazione MySielteID, scaricabile gratuitamente da Google Play per dispositivi mobili Android, App Store per dispositivi Apple e Windows Store per dispositivi con sistema operativo Windows Phone 10 o Windows 10 (vedi i requisiti necessari al paragrafo 7.3.1.1).

L'applicazione consente di utilizzare l'accesso di Livello 2 SPID con un codice OTP a scadenza generato sul proprio dispositivo.

Prima di utilizzare l'applicazione, è necessario effettuare una fase di inizializzazione con la propria identità digitale. Questa fase prevede l'interazione tra l'applicazione e la sezione del proprio profilo SielteID, disponibile tramite l'indirizzo https://profilo.sielteid.it (paragrafo 7.3.3).

L'App, all'avvio, effettua una serie di verifiche, che risultano essere indispensabili per il suo funzionamento. Viene verificato, inizialmente, che la connessione ad Internet del dispositivo risulti attiva; in caso contrario, appare un messaggio di errore, indicante l'impossibilità di utilizzo ed avvio dell'app. Questa verifica avviene nel caso di inizializzazione e associazione dell'app con l'identità digitale dell'utente, quindi al suo primo utilizzo, nella pagina dei servizi preferiti (paragrafo 7.3.1.6), nel caso di cambio del codice di sblocco (paragrafo 7.3.1.7.1) e nel caso di

richiesta di assistenza (paragrafo 7.3.1.8). Durante l'utilizzo successivo all'inizializzazione dell'app (paragrafo 7.3.1.9) e per acquisire il codice OTP (paragrafo 7.3.1.5) non è necessaria la connessione ad Internet. Ulteriore verifica richiesta dall'app è la sincronizzazione del dispositivo con l'ora corrente per far sì che il codice OTP generato risulti utilizzabile nell'intervallo di tempo indicato.

Dopo aver associato l'applicazione, nella sezione SPID Livello 2 all'interno di "Gestione Servizi", l'utente visualizza la "Lista SPID Livello 2" in cui potrà, in qualsiasi momento, controllare lo storico dei dispositivi cellulari e/o tablet associati, con data e orario dell'ultimo utilizzo e, mediante il pulsante  sotto "Azioni" è possibile rimuovere l'associazione.

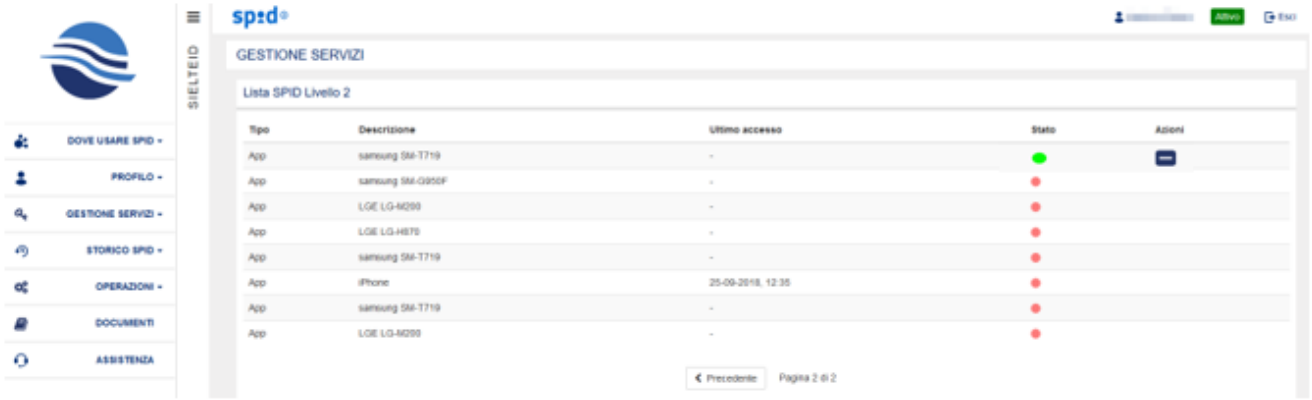


Figura 35- Lista SPID Livello 2

7.3.1.1 REQUISITI

- Android - Versione necessaria Android 4.4 e versioni successive
- iOS - 8.0 o versioni successive (ulteriori informazioni sono disponibili sulla pagina dedicata dello store Apple (https://itunes.apple.com/it/app/mysielteid/).
- Windows - Windows Phone 10, o superiore, o Windows 10, o versione successive.

7.3.1.2 SCHERMATA INIZIALE

Al momento del primo utilizzo dell'applicazione, nella schermata iniziale, l'utente ha la possibilità di poter effettuare l'accesso al proprio profilo SielteID, cliccando sul tasto "Accedi", o, se non l'ha ancora fatto, effettuare la registrazione per ottenere la propria identità digitale, cliccando sul tasto "Registrati" (vedi capitolo 4.1):

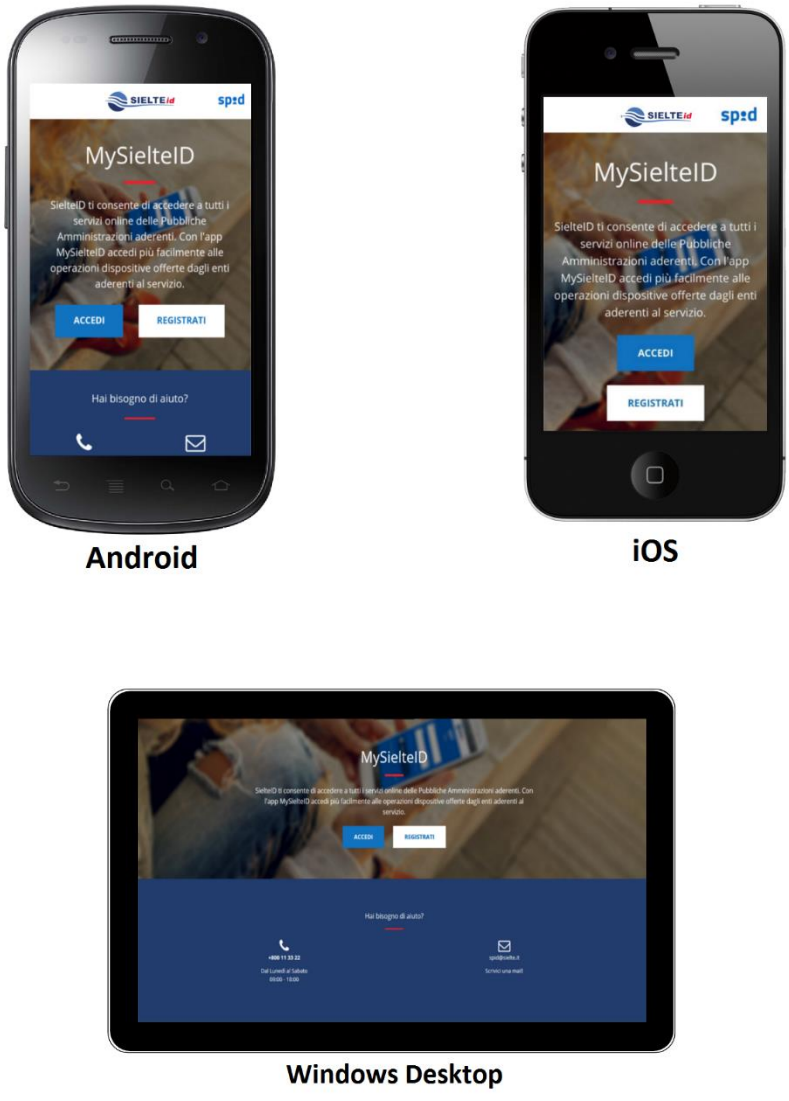


Figura 36 – Schermata iniziale di MySielteID

7.3.1.3 SCHERMATA DI AUTENTICAZIONE

Cliccando su “Accedi”, l’utente viene indirizzato alla pagina di accesso, in cui gli viene richiesto di inserire le proprie credenziali SielteID.

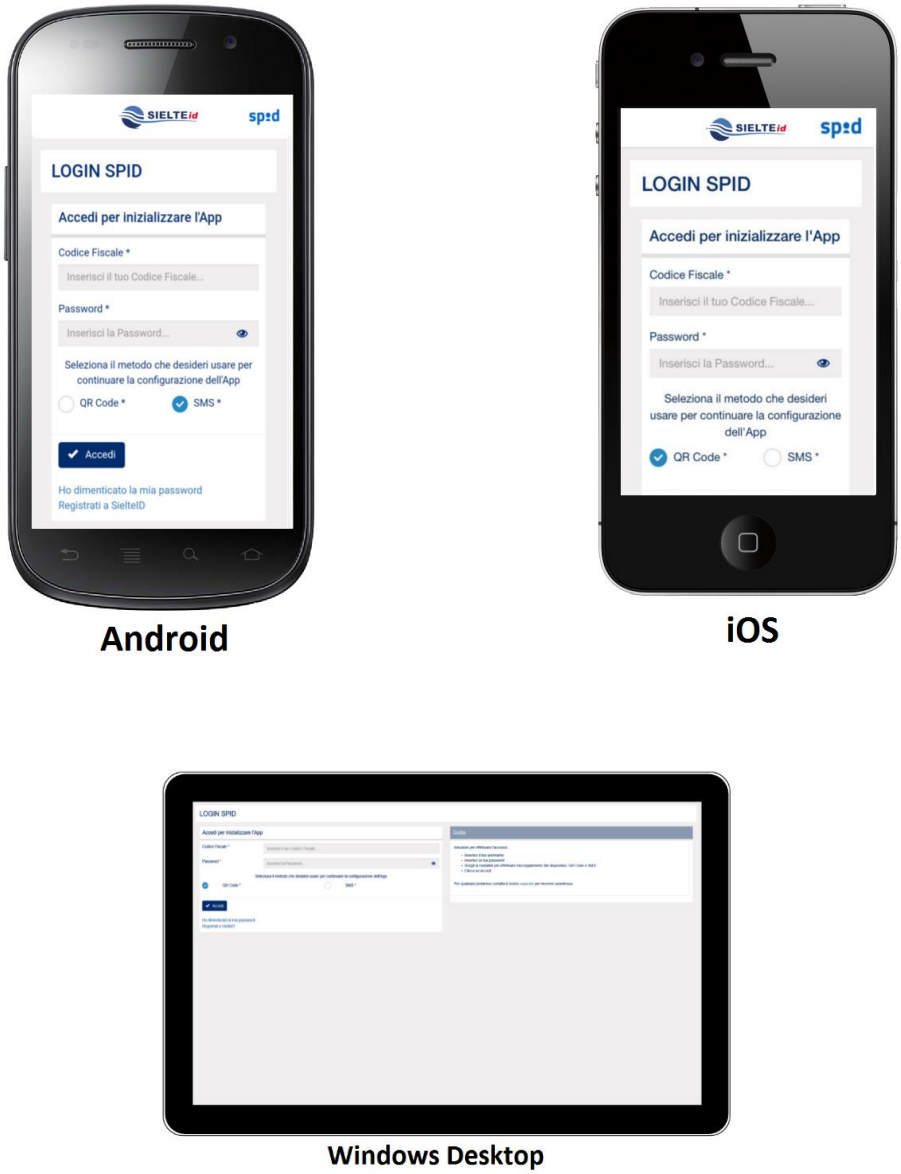


Figura 37 – Schermata di autenticazione di MySielteID

Qui ha, inoltre, la possibilità di poter scegliere quale modalità di associazione utilizzare se tramite QRCode (vedi paragrafo 7.3.1.3.1) o se tramite SMS (vedi paragrafo 7.3.1.3.2).

7.3.1.3.1 SCANNER DEL QRCODE

Se le credenziali vengono inserite correttamente e l'utente ha scelto la modalità QRCode per associare l'app alla propria identità digitale, gli viene richiesto di inquadrare, tramite la camera del proprio dispositivo, il codice QRCode generato, disponibile all'interno di "Aggiungi Servizio", "SPID LIV 2"; occorre quindi accedere al profilo dal proprio PC.

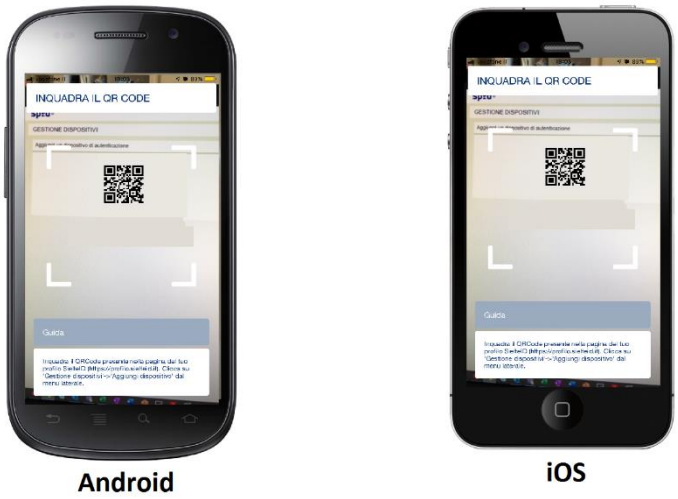


Figura 38 – Schermata per inquadrare il QRCode

7.3.1.3.2 VERIFICA OTP VIA SMS

Se le credenziali vengono inserite correttamente e l'utente ha scelto la modalità SMS per associare l'app alla propria identità digitale, viene indirizzato alla pagina seguente, in cui deve inserire il codice OTP, ricevuto via SMS, al numero di cellulare inserito tra i dati della propria identità digitale.

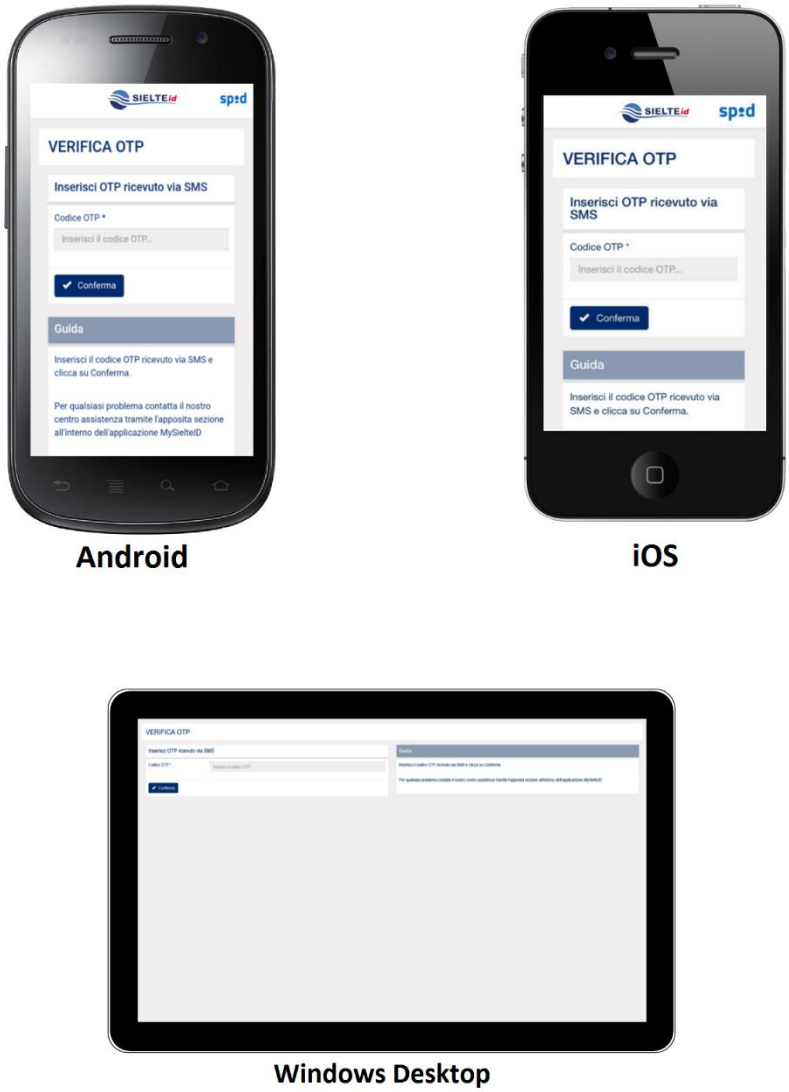


Figura 39 – Schermata di verifica del codice OTP ricevuto via SMS su MySielteID

7.3.1.4 INSERIMENTO DEL CODICE DI SICUREZZA

Conclusa la fase di verifica, viene richiesto all'utente l'inserimento di un codice segreto da utilizzare per proteggere l'applicazione, utile per potervi accedere nel corso di un secondo utilizzo.

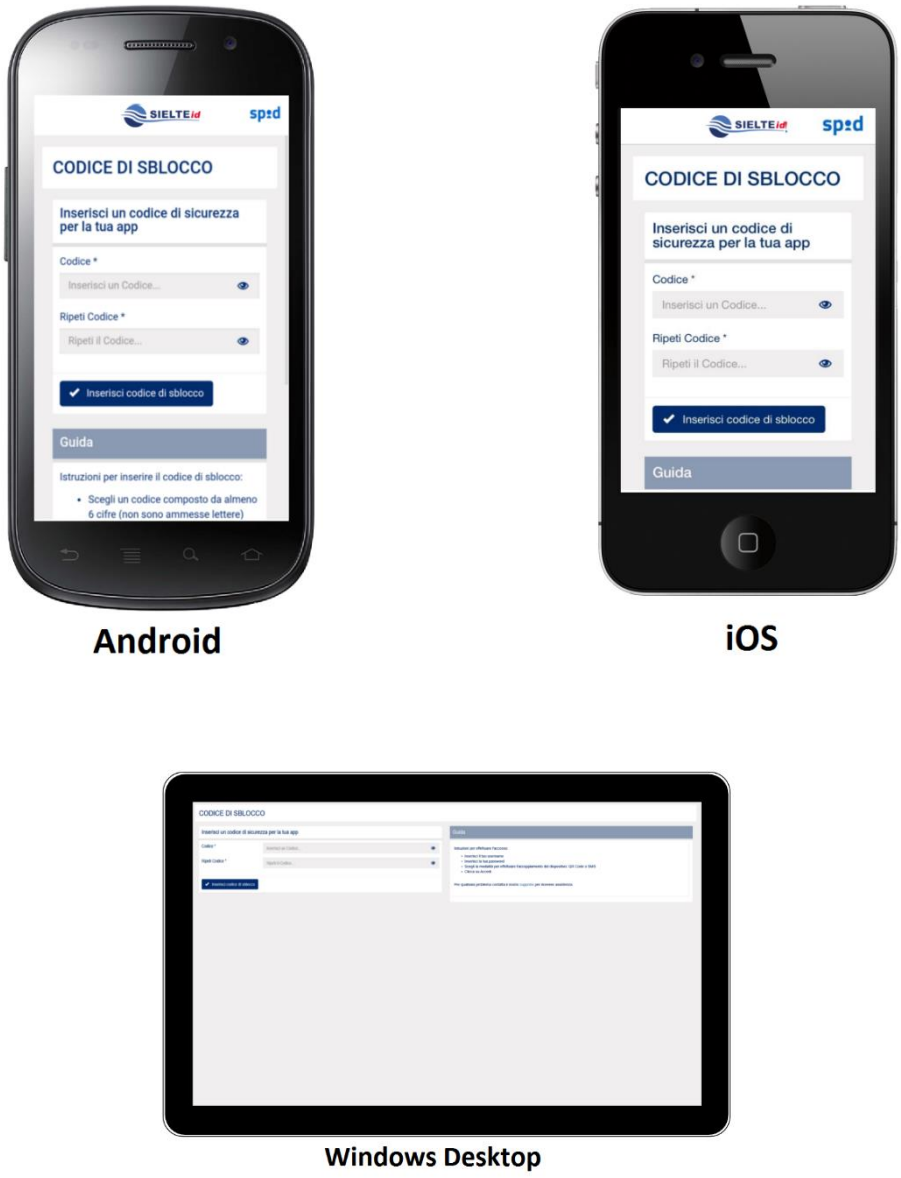


Figura 40 – Schermata di inserimento codice di sblocco di MySielteID

Configurato il codice, sui dispositivi con sistema operativo iOS e Android, che ne siano provvisti, viene chiesto all'utente, se abilitare o meno l'impronta digitale, utile per poter accedere all'app, senza il bisogno di inserire il codice di sblocco.

7.3.1.5 GENERAZIONE DEL CODICE OTP

Successivamente, l'utente può accedere alla pagina di generazione del codice OTP, da utilizzare come secondo fattore, quando viene richiesta l'autenticazione di Livello 2 SPID. In alto a destra dell'OTP, è visibile l'icona, che indica quale account si è scelto di utilizzare e per il quale il codice sia valido.

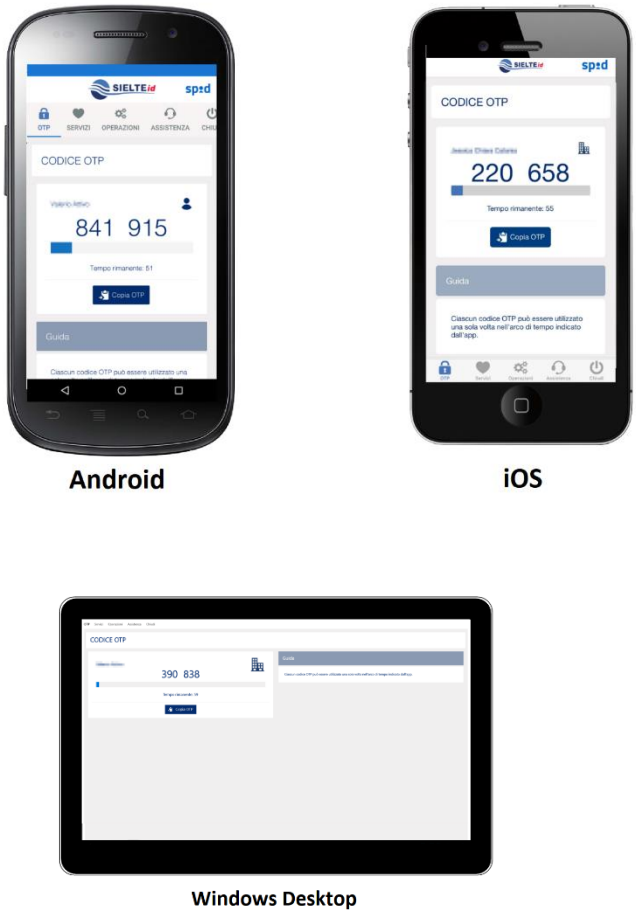


Figura 41 – Schermata di generazione codice OTP di MySielteID

7.3.1.6 LISTA DEI SERVIZI PREFERITI

Mediante il menu "Preferiti", è possibile accedere ai servizi preferiti, scelti tramite la pagina di profilo di SPID. Cliccando su un servizio determinato, si apre la pagina web di riferimento.

Come descritto nel paragrafo 7.1.1, l'utente può scegliere quali servizi aggiungere ai propri preferiti tramite la pagina web del proprio profilo SielteID.

Figura 42 – Schermata dei servizi preferiti di MySielteID

7.3.1.7 OPERAZIONI

Tramite il menu "Operazioni", è possibile accedere: alle funzionalità relative all'App, quali il cambio del codice di sicurezza (vedi paragrafo 7.3.1.7.1), attivazione/disattivazione

dell'impronta digitale e disconnessione dell'account; alle funzionalità relative al proprio profilo SielteID, quali cambio della password e aggiornamento dei documenti e documentazione ufficiale. L'operazione "Disconnetti account" richiede di ripetere il processo di associazione del dispositivo alla propria identità digitale.

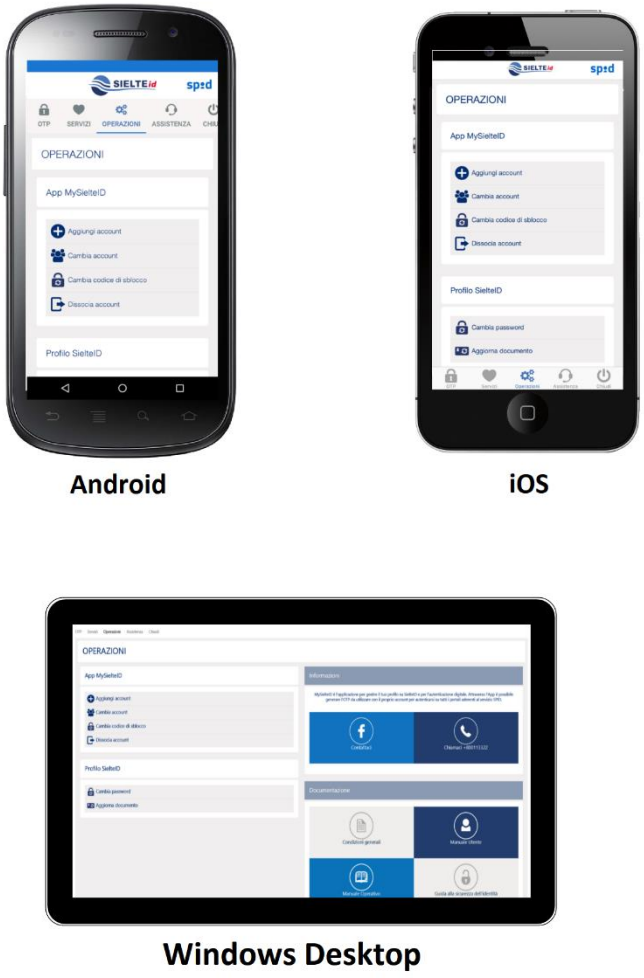


Figura 43 – Schermata delle operazioni disponibili su MySielteID

7.3.1.7.1 CAMBIO DEL CODICE DI SBLOCCO

Cliccando su “Cambio codice di sblocco”, all’interno del menu “App MySielteID”, l’utente può effettuare l’operazione di modifica del codice di sicurezza, inserito in fase di inizializzazione, compilando i rispettivi campi con il codice vecchio e con quello nuovo.

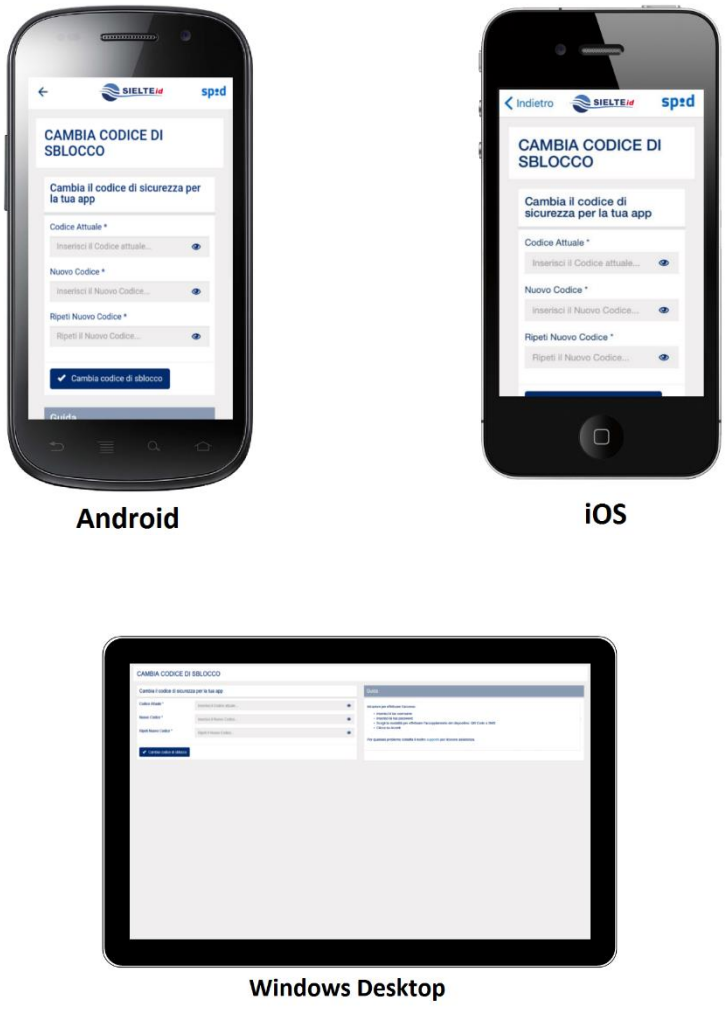


Figura 44 – Schermata di cambio codice di sblocco di MySielteID

7.3.1.7.2 CAMBIO PASSWORD

Cliccando su “Cambio password”, all’interno del menu “Profilo SielteID”, l’utente può effettuare l’operazione di cambio password, inserendo la vecchia password utilizzata e quella nuova.

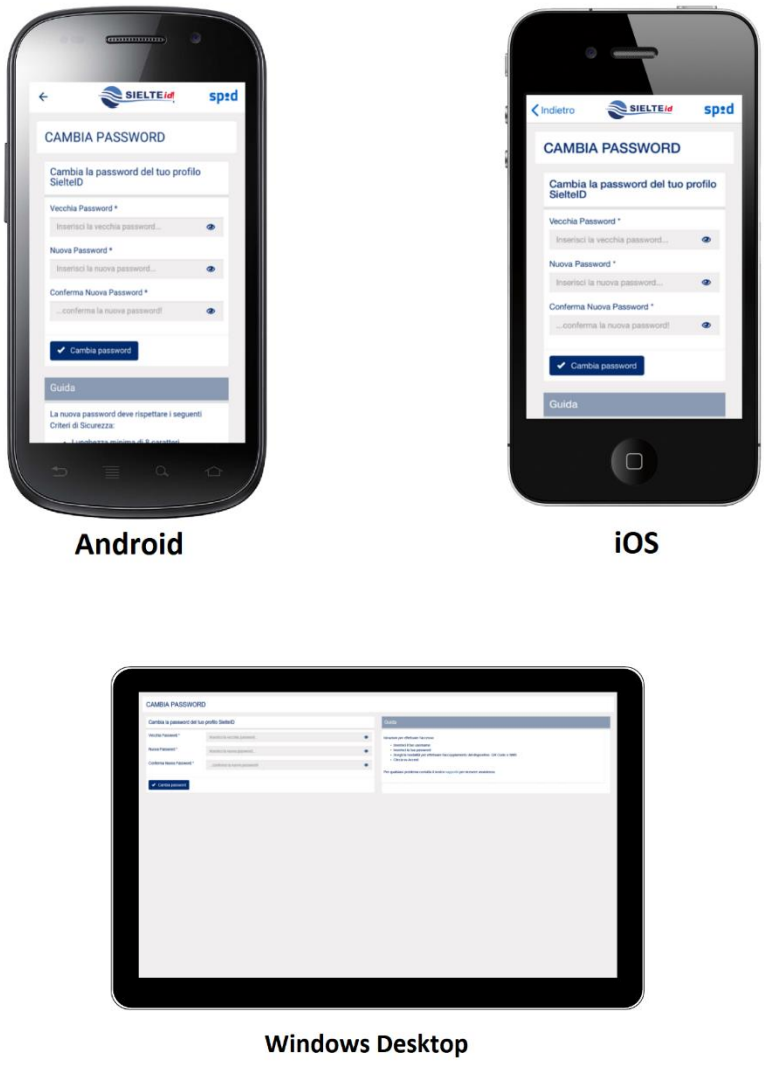


Figura 45 – Schermata di cambio password del profilo SielteID, da app MySielteID

7.3.1.7.3 AGGIORNA DOCUMENTO

Cliccando su “Aggiorna documento”, all’interno del menu “Profilo SielteID”, l’utente può procedere con l’operazione di aggiornamento dei propri documenti, inserendo i dati richiesti e caricandone le scansioni.

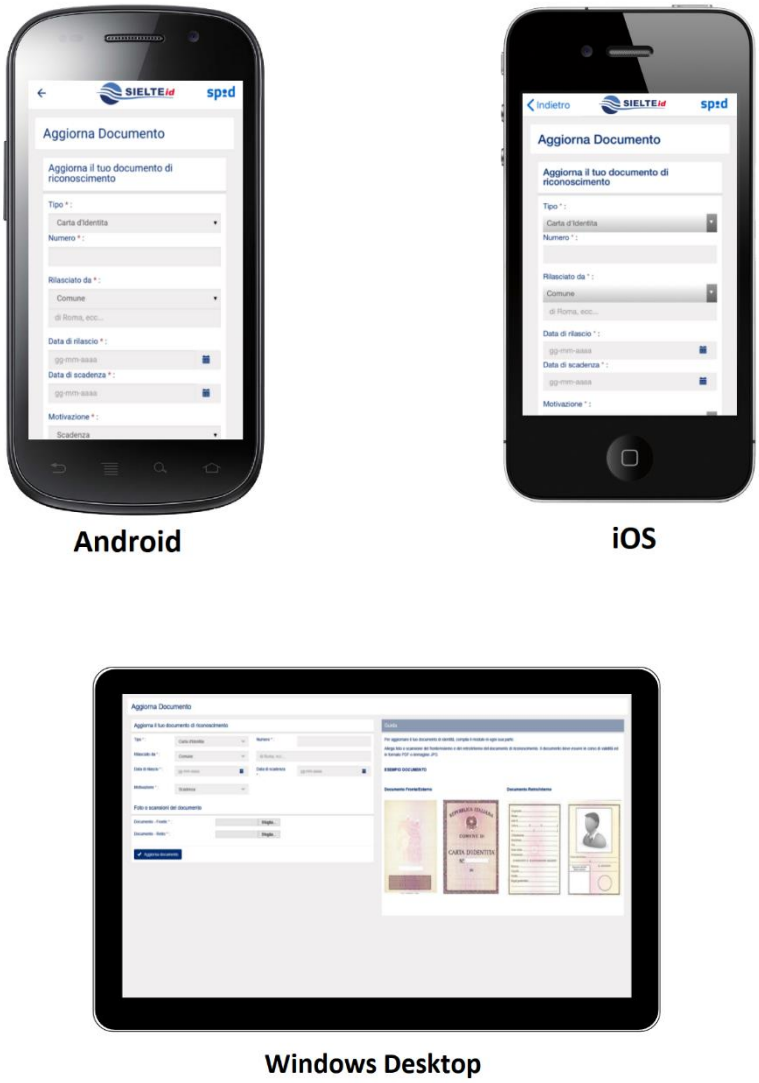


Figura 46 – Schermata di aggiornamento documenti all’interno dell’app MySielteID

7.3.1.8 ASSISTENZA

Cliccando su “Assistenza”, l’utente può inviare una richiesta di supporto all’assistenza dedicata di Sielte.

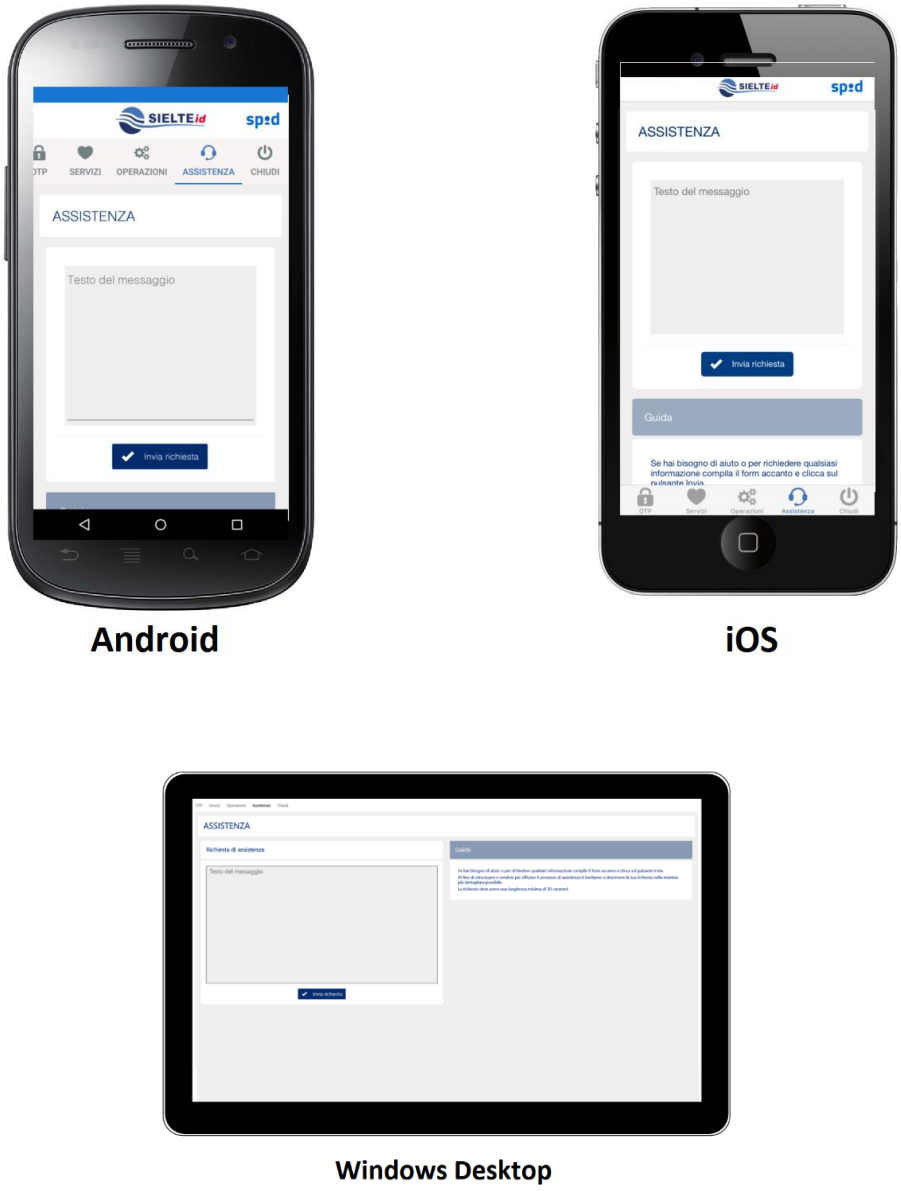


Figura 47 – Schermata della richiesta di assistenza su MySielteID

7.3.1.9 ACCESSO PER NUOVO UTILIZZO DELL'APP MYSIELTEID

Conclusa la fase di attivazione dell'App, è possibile utilizzare nuovamente l'applicazione, effettuando nuovamente l'accesso, digitando il codice di sicurezza, inserito in fase di configurazione o, nel caso di attivazione, tramite impronta digitale.

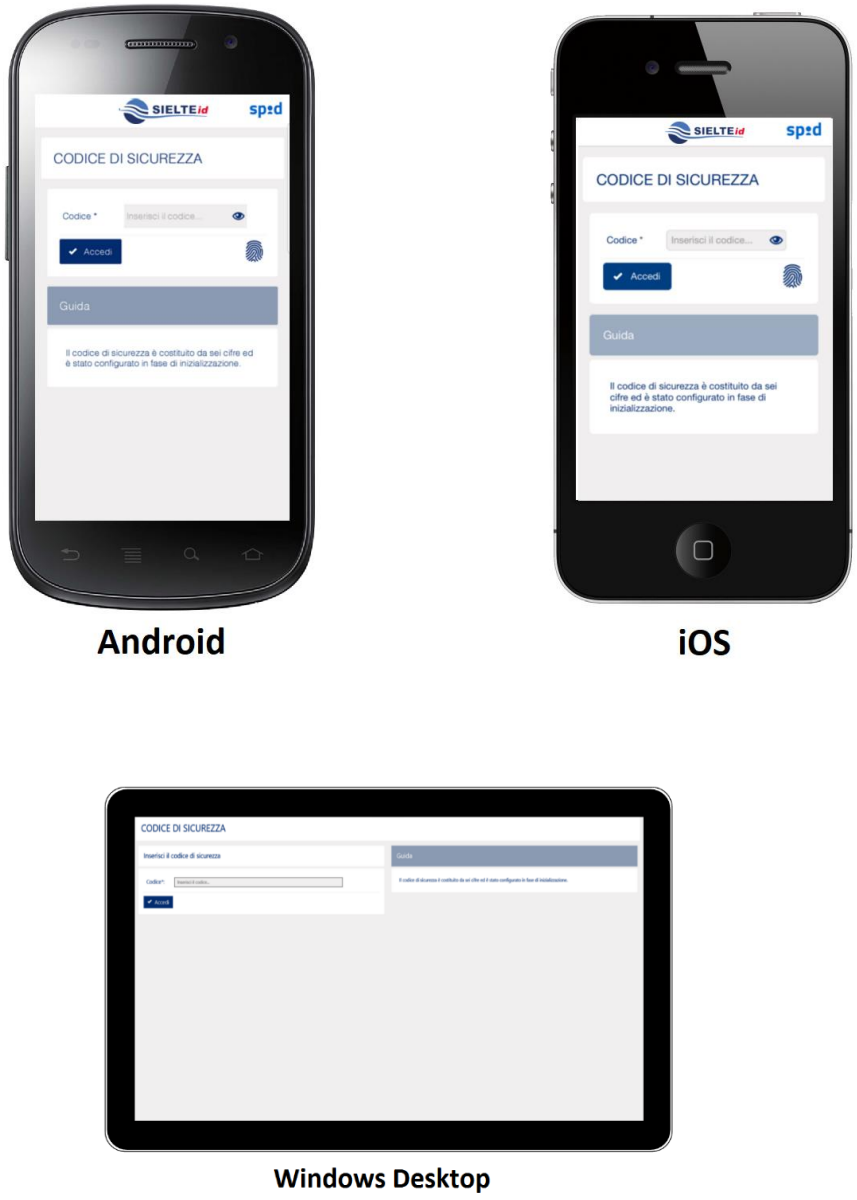


Figura 48 – Schermata di accesso all'app MySielteID, dopo la fase di inizializzazione

Qualora venisse effettuato l'accesso tramite un altro dispositivo, il token, cui è associato il dispositivo precedentemente attivato, viene disabilitato in automatico.

7.3.1.10 MULTIUTENZA

All'interno del menu operazioni, cliccando su "Cambia account", viene mostrata la lista degli account configurati su quel dispositivo; qualora ci sia più di un account configurato, la lista apparirà anche dopo che l'utente ha effettuato l'accesso, permettendogli di scegliere l'utenza da utilizzare.

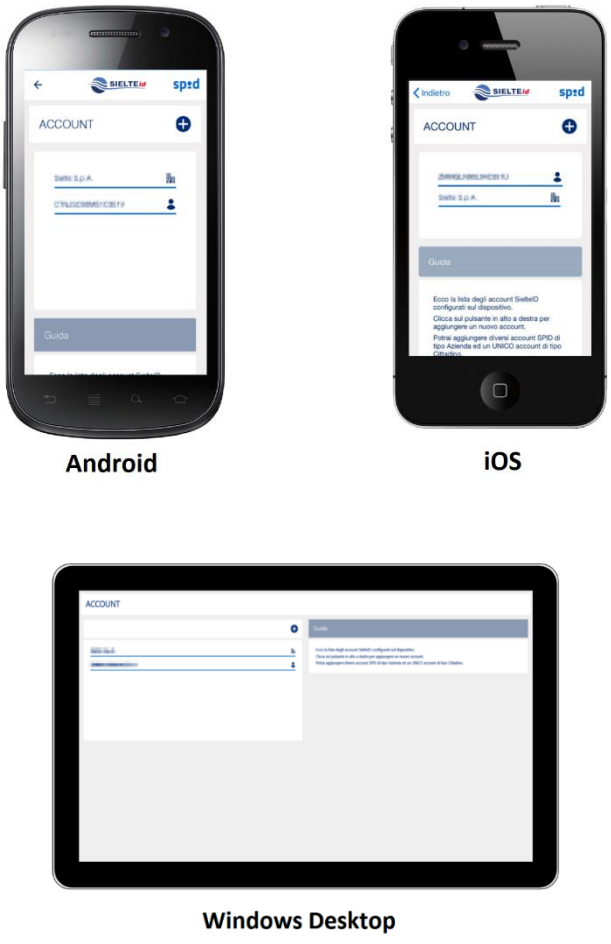


Figura 49 – Lista di account configurati nell'app MySielteID

Cliccando sul pulsante ⊕ l'utente può aggiungere ulteriori account; per aggiungere una nuova utenza dovrà eseguire nuovamente il processo di inizializzazione dell'app e inserire un ulteriore codice di sblocco, che verrà associato al nuovo account. Per l'accesso all'app e l'utilizzo di diversi account, quindi, saranno necessari pin diversi.

7.3.1.11 NOTIFICHE

Gli utenti che avranno configurato l'app correttamente, potranno utilizzare le notifiche come ulteriore metodo di autenticazione, consentendone il permesso sul dispositivo. Cliccando sulla notifica ricevuta, potranno scegliere se autorizzare l'accesso di secondo livello ai servizi SPID, come in figura.

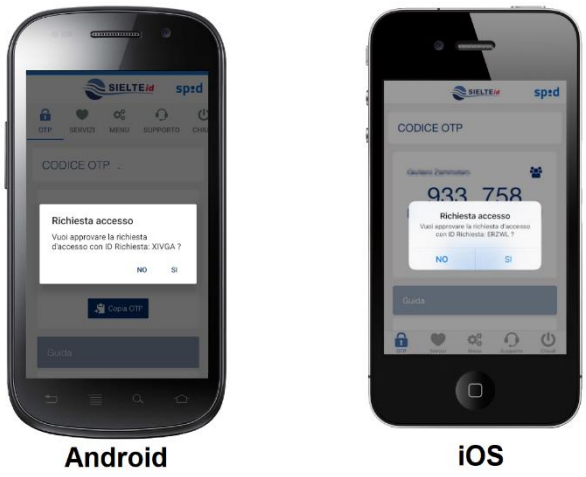


Figura 50 – Ricezione notifica nell'app MySielteID

7.3.2 *Spid LIV 3*

Sielte mette a disposizione degli utenti che hanno ottenuto la propria identità digitale con SielteID di attivare il Livello 3 di autenticazione. Prima di poter accedere ai servizi di Livello 3, è necessario effettuare la fase di associazione del dispositivo digitale tramite la smart card, dalla sezione del proprio profilo SielteID, disponibile collegandosi sul proprio profilo personale all'indirizzo https://profilo.sielteid.it.

Tramite la voce Aggiungi Servizio è possibile aggiungere il dispositivo smartcard selezionando il tipo di Servizio "SPID Livello 3":

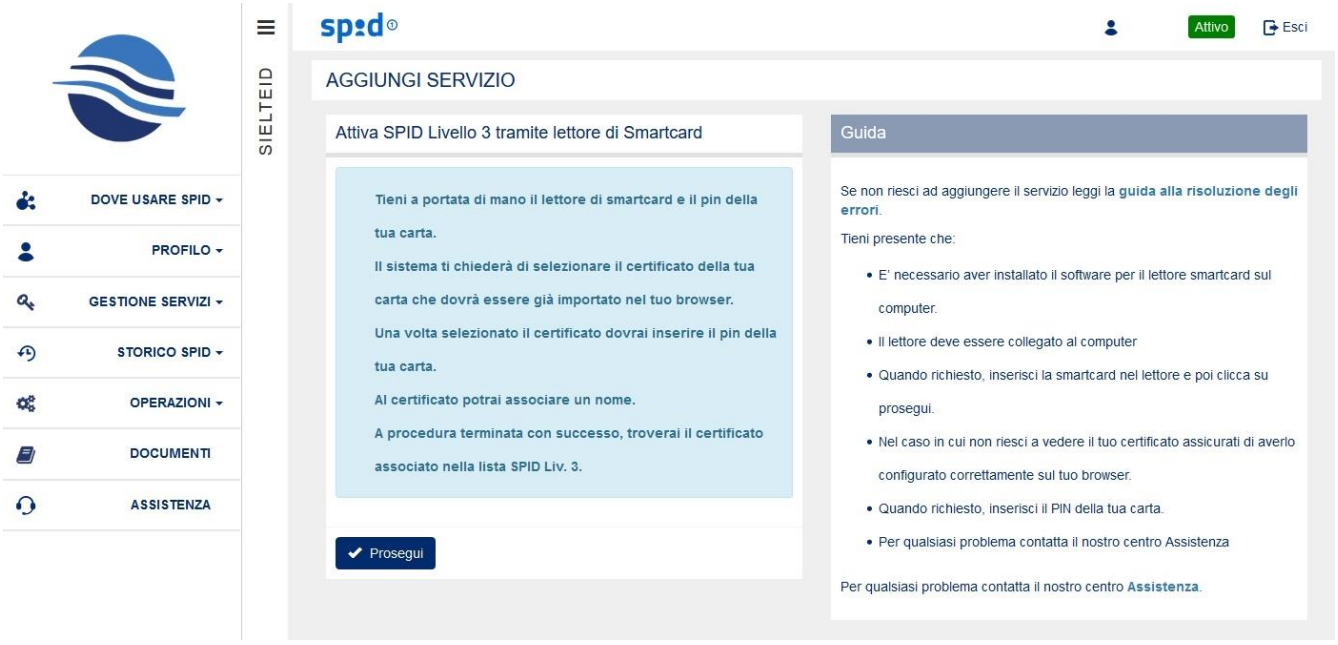


Figura 51- Attiva SPID Livello 3

Cliccando su "Prosegui", è necessario selezionare il certificato inserito nella smartcard

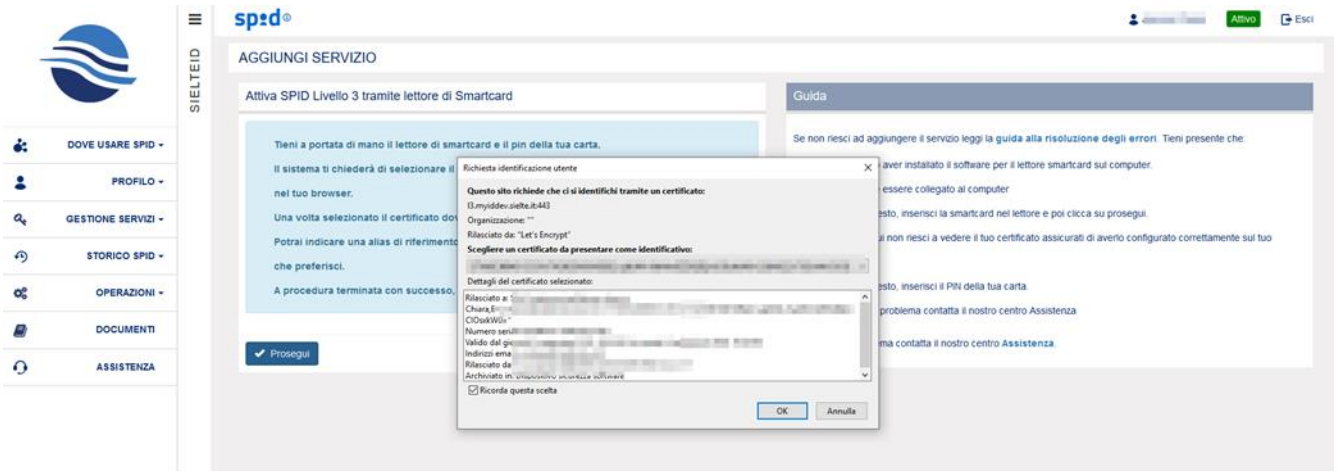


Figura 52- Selezione certificato

Successivamente va inserito il pin e, se il processo va a buon fine, è necessario aggiungere il nome del certificato:

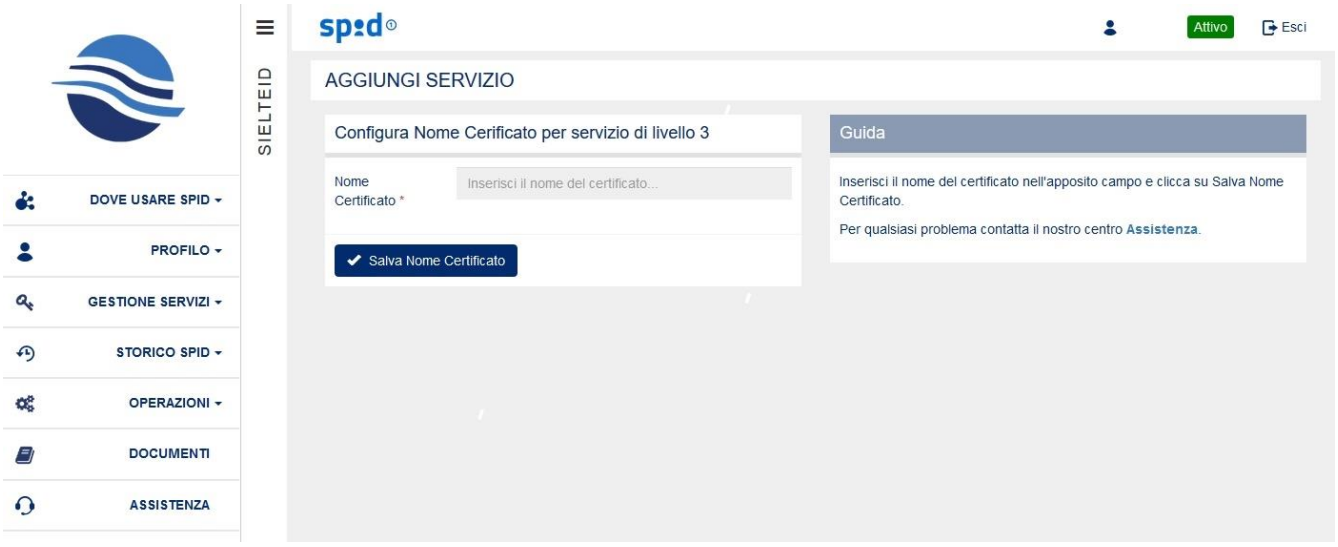


Figura 53- Configura Nome Certificato

Dopo aver associato il dispositivo smartcard, sempre nella stessa sezione, l'utente vedrà di seguito la "Lista SPID Livello 3" in cui potrà in qualsiasi momento controllare lo storico dei dispositivi che ha associato al profilo con il nome certificato prescelto, la sua validità, il suo stato e la possibilità di rimuovere l'associazione tramite il pulsante presente sotto "Azioni".

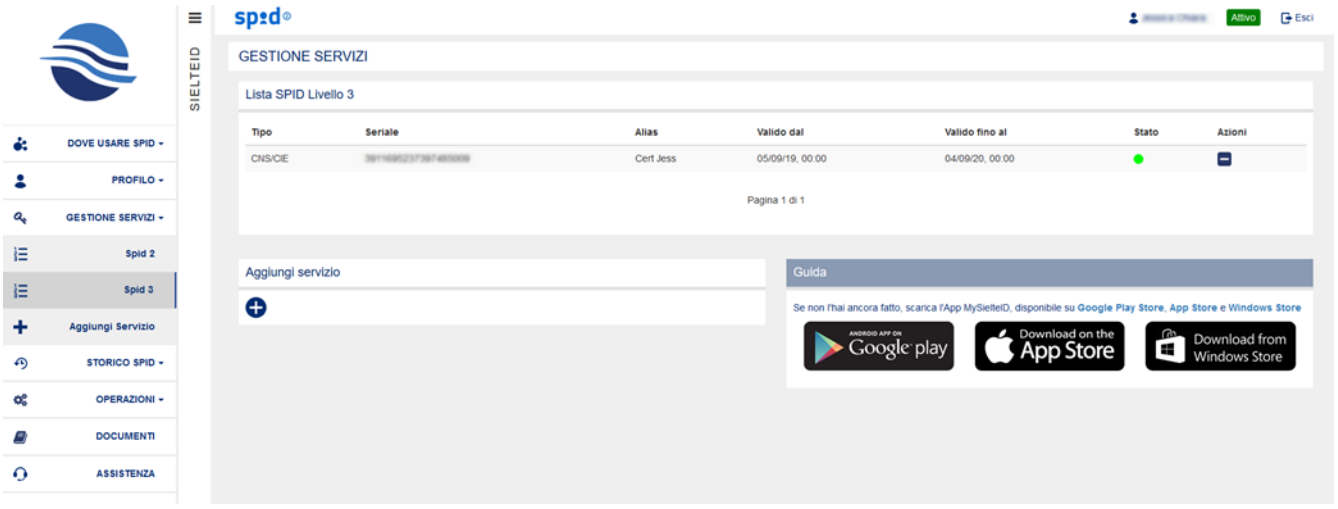


Figura 54- Lista SPID Livello 3

7.3.3 *Aggiungi Servizio*

Cliccando su “Aggiungi Servizio”, all’interno di “Gestione Servizi”, se non ancora attive, viene proposto di attivare le credenziali di livello 2 tramite app (gratuitamente), oppure le credenziali di Livello 3. Per procedere su “Aggiungi Servizio” è necessario accedere con livello 2 tramite codice OTP ricevuto via SMS.

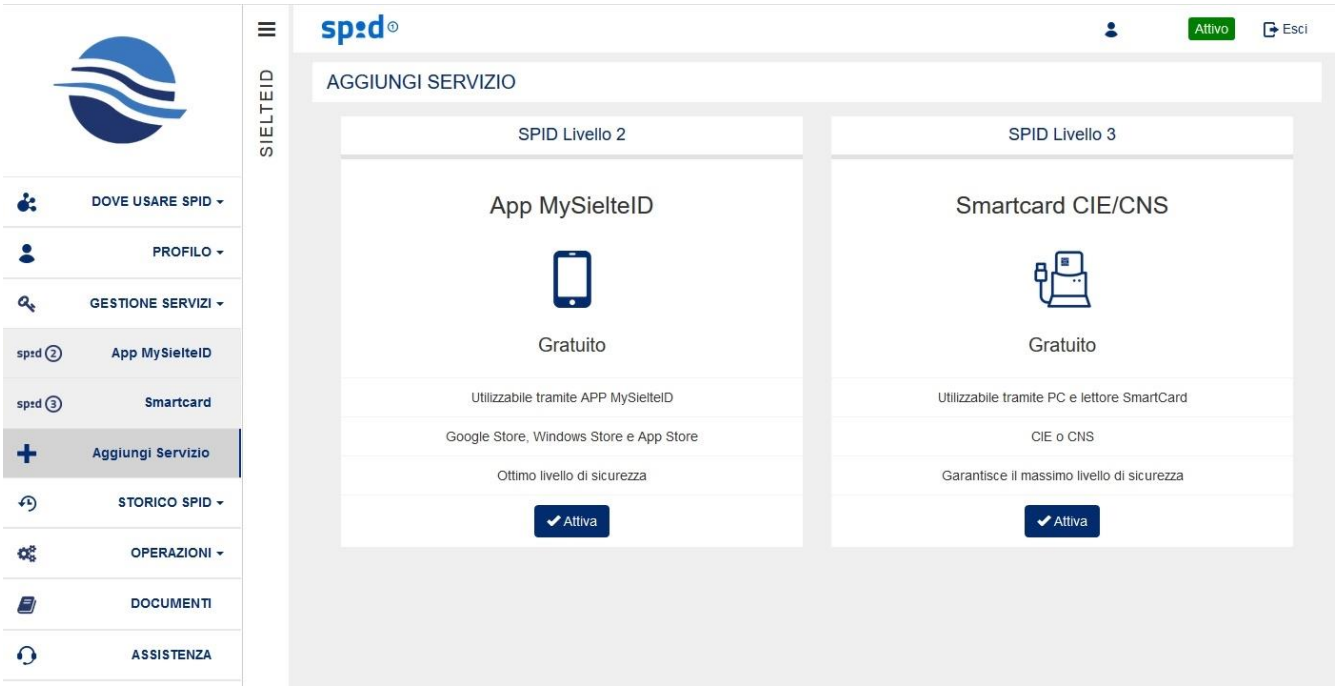


Figura 55- Aggiungi servizio

Cliccando su Attiva nella sezione SPID Livello 2, viene generato il QRCode da associare al dispositivo (come in Figura):

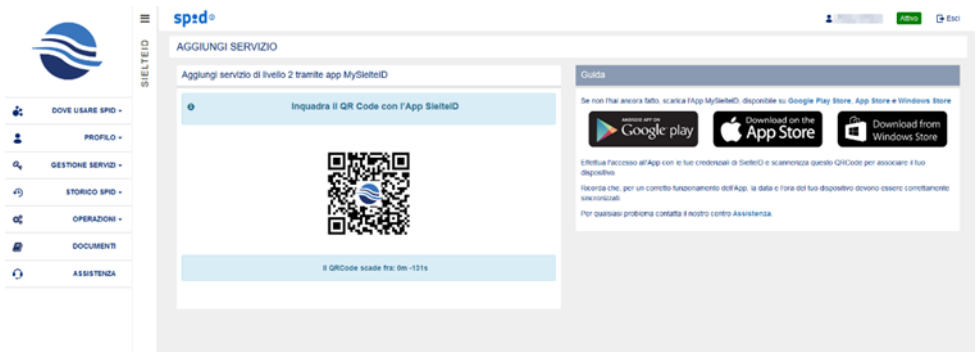


Figura 56- Interfaccia generazione QRCode

Cliccando su Attiva nella sezione SPID Livello 3 è possibile aggiungere il dispositivo smartcard come spiegato precedentemente.

7.4 Storico SPID

7.4.1 *Storico accessi*

Cliccando su “Storico accessi”, all’interno della voce “Storico SPID”, l’utente può visualizzare l’elenco dello storico accessi effettuati tramite l’identità digitale SPID, filtrandoli mediante opportune opzioni tra le quali ad esempio, l’intervallo di tempo desiderato ed il livello di accesso (se di tipo 1 o 2 o 3).
Questa operazione richiede un’autenticazione di livello 2, come spiegato successivamente al capitolo 8.

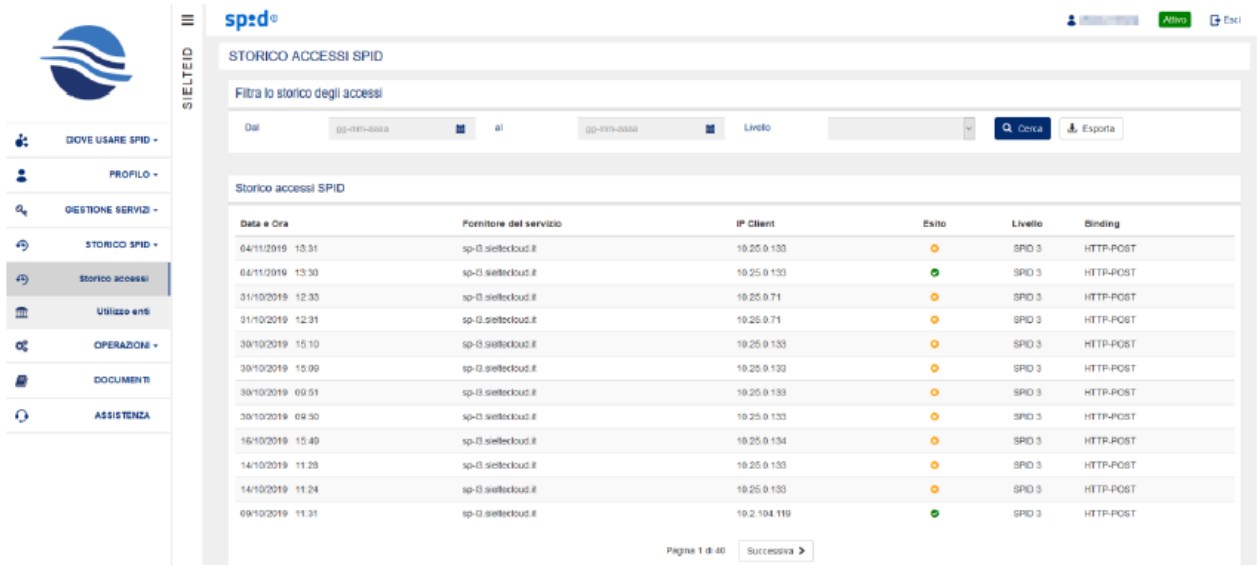


Figura 57 – Interfaccia dello storico accessi

Nell’elenco presente all’interno della figura 57 sono riportate le informazioni riguardanti la data e l’ora di accesso, il fornitore del servizio con cui è stato effettuato l’accesso, l’indirizzo IP del dispositivo dell’utente, l’esito dell’accesso, il livello di sicurezza utilizzato ed il Binding.

Passando il puntatore del mouse sopra l’icona dell’esito, appare la relativa descrizione.

L'utente, inoltre, può esportare i dati di tali informazioni filtrate, così da poterle memorizzare.

7.4.2 *Utilizzo enti*

Cliccando su "Utilizzo enti", all'interno della voce "Storico SPID", l'utente può visualizzare l'elenco dello storico accessi corrente, effettuati tramite l'identità digitale SPID, organizzato per enti, aggiornato tramite statistiche e filtrati tramite opportune opzioni, tra le quali ad esempio, l'intervallo di tempo desiderato ed il livello di accesso (se di tipo 1 o 2 o 3).

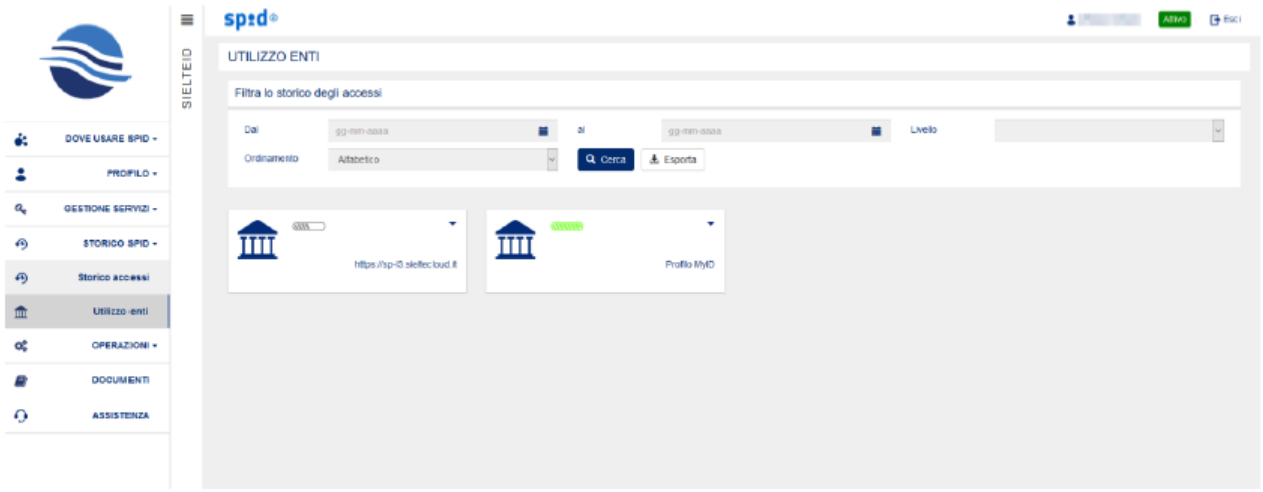


Figura 58 – Interfaccia dello storico utilizzo enti

Nell'elenco presente in figura 58 sono riportate le informazioni riguardanti la data e l'ora di accesso, il fornitore del servizio, cui è stato effettuato l'accesso, l'indirizzo IP del dispositivo dell'utente, l'esito dell'accesso, il livello di sicurezza utilizzato ed il Binding.

L'utente, inoltre, può esportare i dati di tali informazioni filtrate, così da poterle memorizzare.

Questa operazione richiede un'autenticazione di livello 2, vedi capitolo 8.

7.5 Operazioni

All'interno dell'area personale è possibile accedere alla pagina "Operazioni" per la gestione delle credenziali dell'identità digitali, dove è possibile:

- Modificare la password di accesso (prima della data di scadenza).
- Modificare il numero di cellulare.
- Modificare l'indirizzo mail.
- Aggiornare i propri documenti.
- Richiedere la sospensione dell'identità digitale.
- Richiedere la revoca dell'identità digitale.

Tali operazioni richiedono un accesso di livello 2, vedi capitolo 8.

7.5.1 *Cambia password*

Per effettuare il cambio password, l'utente accede alla sezione "Cambia Password", all'interno di "Operazioni", ed inserisce nei campi dedicati (vedi Figura 59 – Interfaccia di cambio password) la vecchia password, la nuova password e la conferma della nuova password per verificarne il corretto inserimento. La nuova password dovrà rispettare i criteri di sicurezza descritti nella guida a fianco. Quando l'utente conferma la modifica cliccando su "Cambia password", il sistema verifica la validità delle informazioni inserite e, in caso di verifica positiva, ne notifica l'esito.

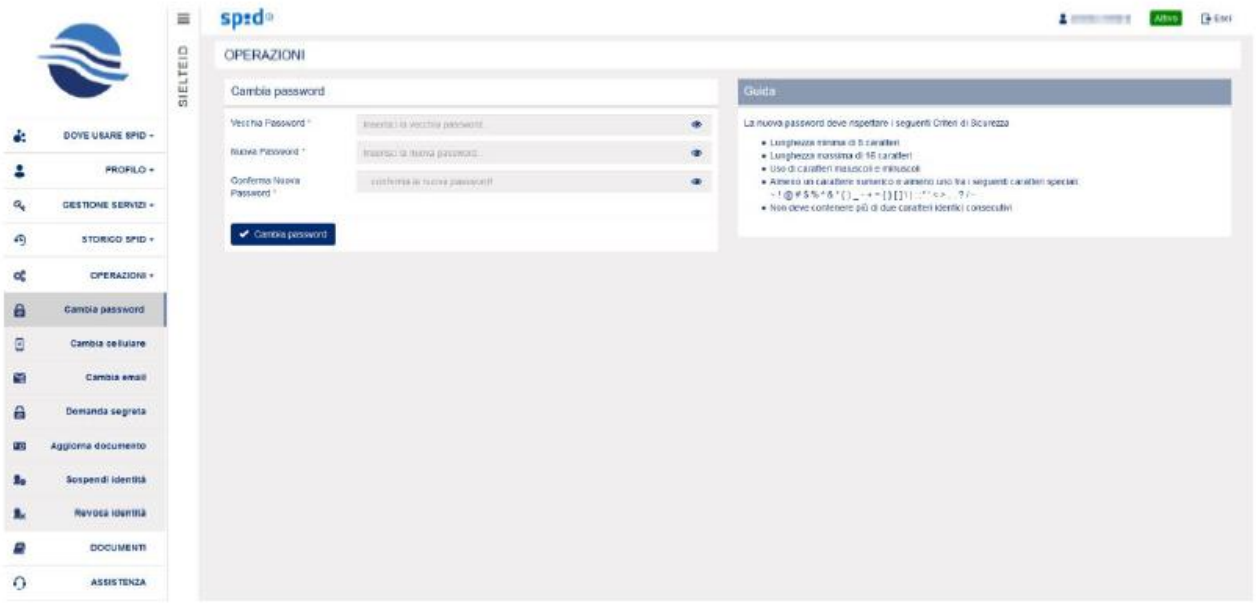


Figura 59 – Interfaccia di cambio password

Inoltre, la password ha una scadenza; l'utente viene avvisato preventivamente di ciò ed ha la possibilità di rinnovarla direttamente dalla propria area personale. Nel caso di scadenza della password questa non potrà più essere utilizzata e quindi l'utente dovrà eseguire il rilascio di nuove credenziali.

7.5.2 *Cambia cellulare*

Per effettuare il cambio del numero di telefono è disponibile la funzione “Cambia cellulare”, all’interno dell’area riservata. Per effettuare la sostituzione del numero di telefono è necessario eseguire la procedura di verifica del nuovo numero.

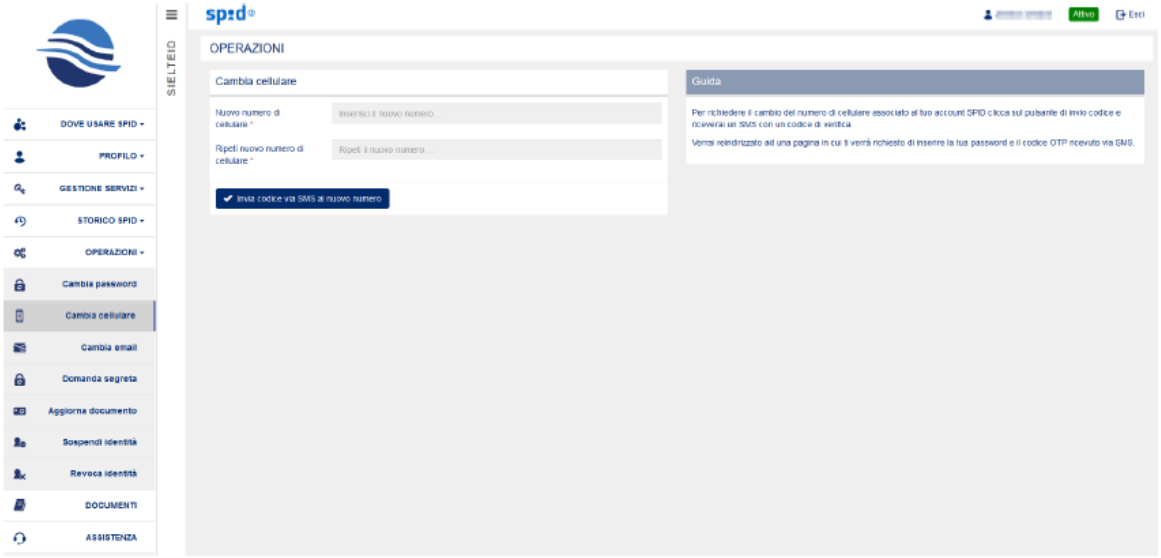


Figura 60 – Interfaccia di cambio numero di cellulare

7.5.3 *Cambio e-mail*

Per effettuare la modifica dell’indirizzo di posta elettronica, l’utente accede alla sezione “Cambia e-mail” ed inserisce nei campi dedicati (vedi Figura 61 – Interfaccia di cambio indirizzo e-mail) il nuovo indirizzo. Quando l’utente conferma la modifica cliccando su “Invia mail di conferma”, il sistema invia una mail con tale richiesta di modifica al nuovo indirizzo di posta elettronica dell’utente contenente un link di conferma.

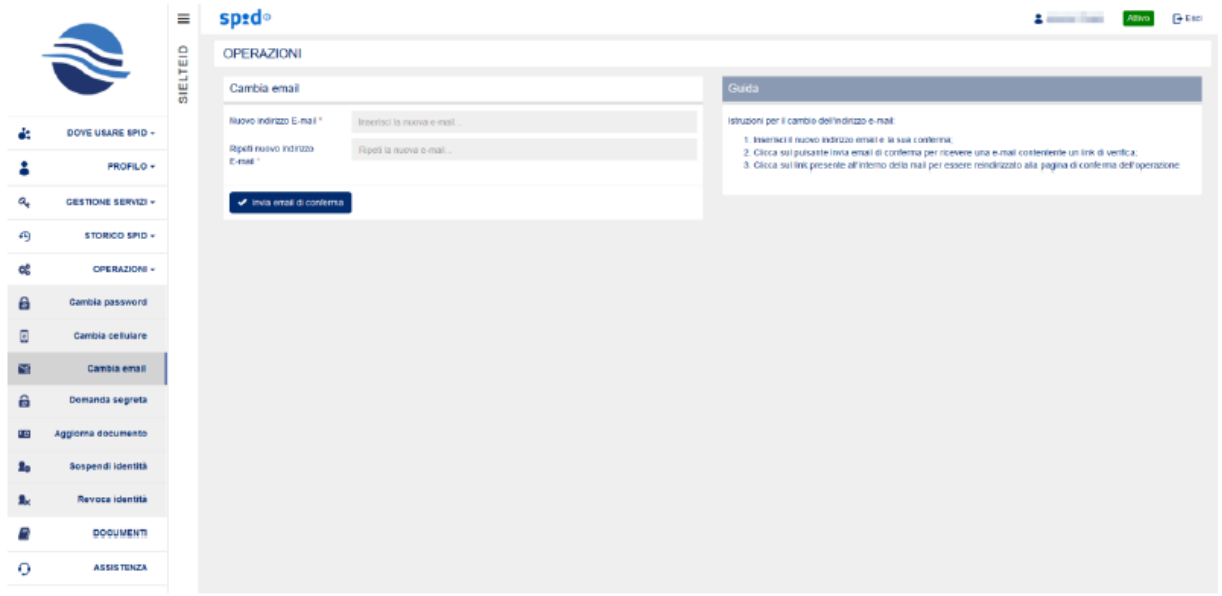


Figura 61 – Interfaccia di cambio indirizzo e-mail

7.5.4 *Domanda segreta*

Alla voce di menu “Domanda Segreta” presente sul proprio profilo, all’interno di Operazioni, l’utente ha la possibilità di modificare la domanda segreta precedentemente impostata.

Per modificarla, basta cliccare sul menu a tendina che appare, scegliere una domanda dalla lista di quelle disponibili, inserire la risposta e confermarla.

A questo punto, cliccando su Salva, viene impostata correttamente una nuova domanda segreta.

È importante per l’utente memorizzare con cura la risposta alla domanda segreta, perché è necessaria per recuperare le credenziali SPID in caso di smarrimento.

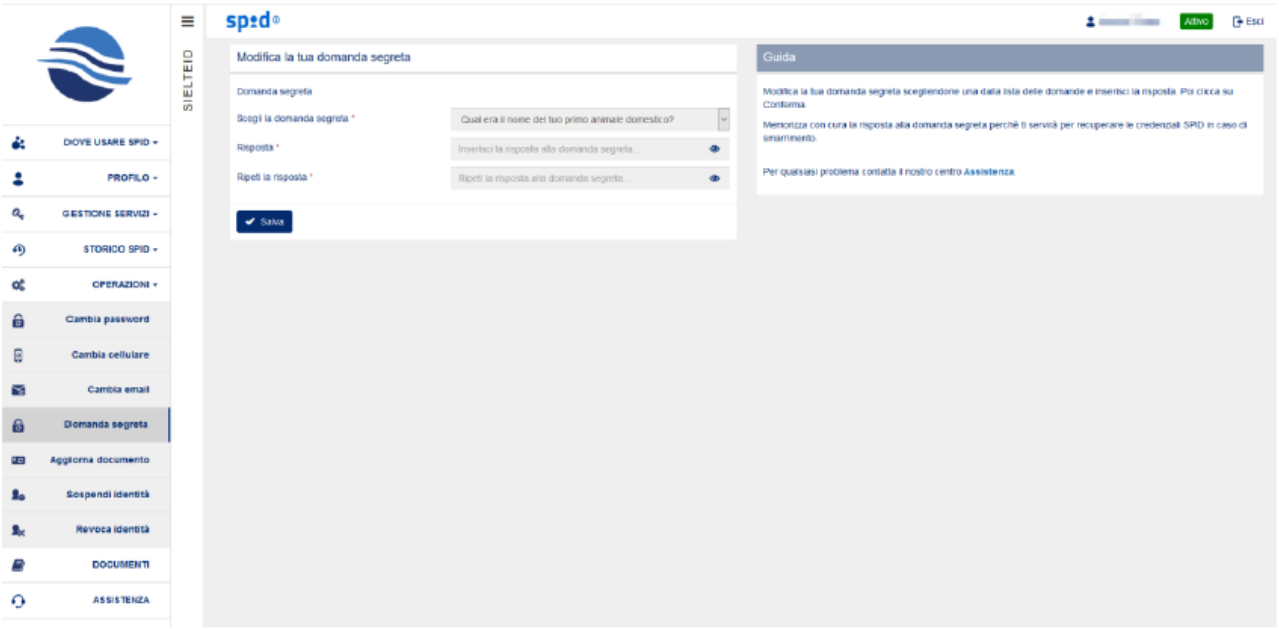


Figura 62 – Interfaccia di modifica domanda segreta

7.5.5 *Aggiorna documento*

Per effettuare l'aggiornamento del proprio documento di riconoscimento scaduto, è possibile accedere alla voce di menu "Aggiorna Documento" presente sul proprio profilo.

Viene richiesto l'inserimento dei dati associati al nuovo documento di identità e viene richiesto di allegare foto o scansione del fronte e del retro del documento di riconoscimento. Il documento deve essere in corso di validità ed in formato PDF o immagine JPG.

Successivamente, viene effettuata la validazione da parte del personale SielteID e, laddove i documenti siano in corso di validità, vengono approvati.

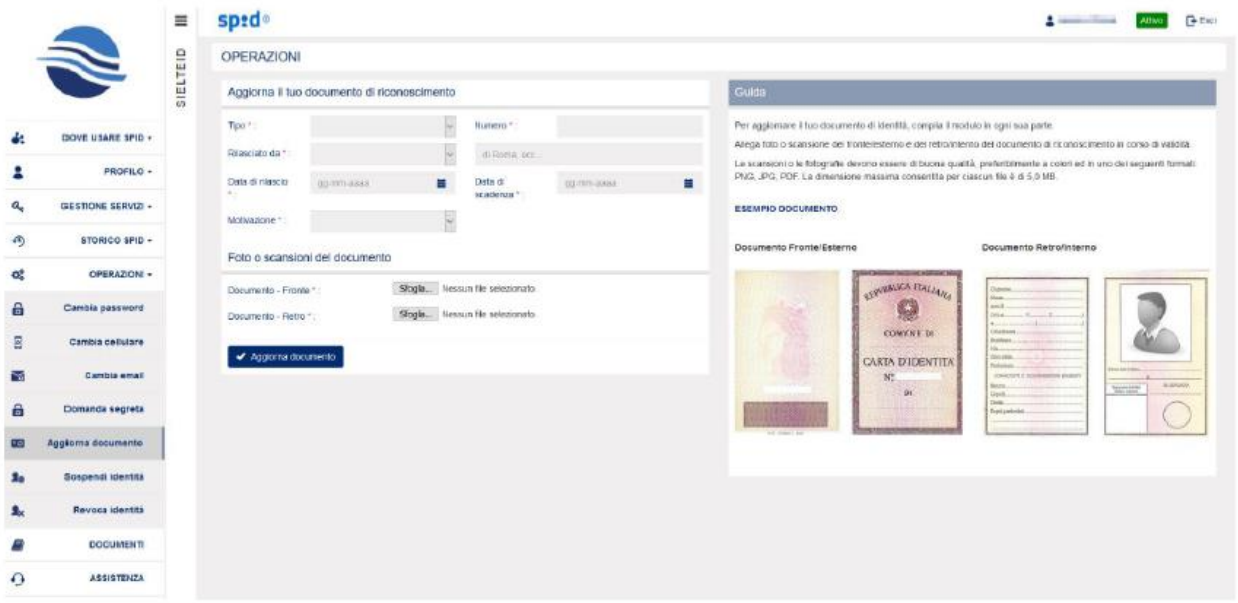


Figura 63 – Interfaccia di aggiornamento documento

7.5.6 *Sospensione e Revoca*

Il cittadino può sospendere la propria identità digitale, per un determinato periodo definito da lui stesso, o richiederne la Revoca definitiva.

Per effettuare l'operazione di "Sospensione" l'utente:

- Sceglie dal menu l'operazione "Sospendi Identità".
- Inserisce la data fino a cui si desidera sospendere il proprio account SPID.
- Inserisce la propria "Password".
- Inserisce il "Codice segreto di Sospensione" ricevuto in fase di attivazione delle credenziali.
- Inserisce la motivazione della richiesta della sospensione (furto, smarrimento, sospetto uso abusivo o altro).
- Per conferma, clicca su "Sospendi Identità".

Quando l'utente conferma la richiesta di sospensione, il sistema verifica la validità delle informazioni inserite e, in caso positivo, presenta un messaggio di conferma della sospensione dell'identità digitale. Automaticamente anche le credenziali associate verranno aggiornate in modalità "sospese" e all'utente viene notificata la corretta sospensione e l'eventuale codice da utilizzare per rimuovere la sospensione.

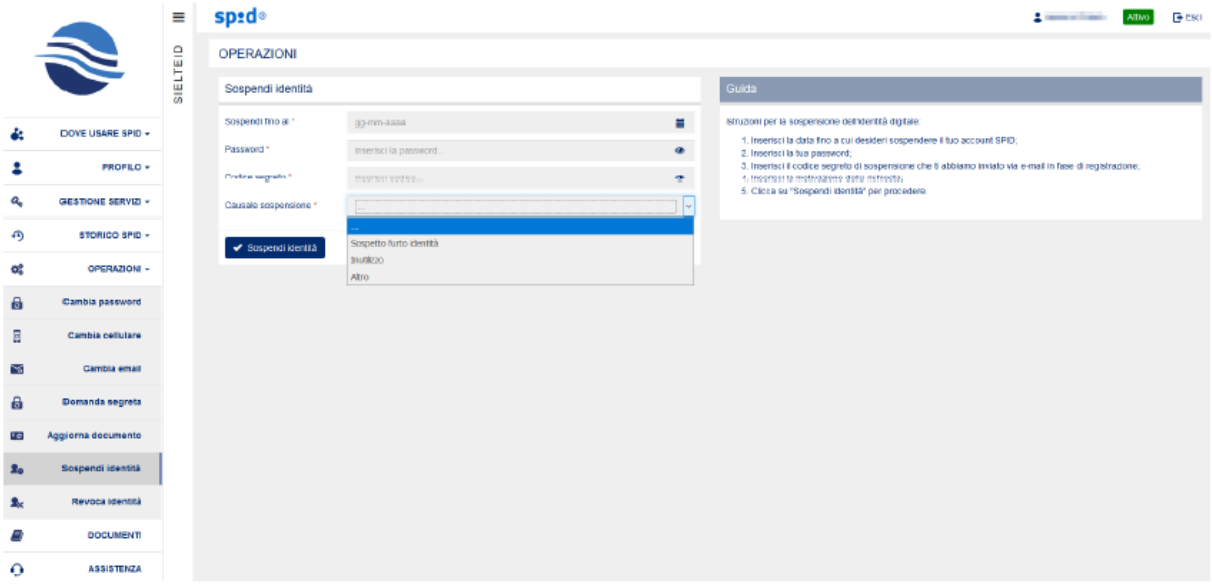


Figura 64 – Interfaccia di sospensione dell'identità digitale

La richiesta di sospensione può essere annullata utilizzando lo stesso servizio disponibile sul sito web.

Per effettuare la richiesta di sblocco sospensione l'utente deve:

- inserire il proprio codice personale identificativo;
- scegliere dal menu a tendina l'operazione "Sblocco Sospensione Identità Digitale";
- inserire il codice di sblocco ricevuto durante l'operazione di sospensione;
- inserire la motivazione della richiesta di sospensione.

Quando l'utente conferma l'operazione, il sistema verifica la validità delle informazioni inserite e, in caso positivo, presenta un messaggio di conferma dello sblocco sospensione dell'identità digitale.

La Revoca dell'identità digitale può essere richiesta dall'utente. Per effettuare la richiesta di "Revoca dell'Identità Digitale" l'utente:

- Sceglie dal menu l'operazione "Revoca Identità".

- Allega copia del proprio documento di riconoscimento valido; nel caso di Furto o Smarrimento, allega copia per immagine della denuncia di smarrimento/furto.
- Inserisce il codice segreto di revoca, inviato via mail in fase di attivazione delle credenziali.
- Inserisce la motivazione della richiesta di revoca (Furto, Smarrimento, Sospetto Uso Abusivo, Altro).
- Clicca per conferma su “Invio richiesta di Revoca”.

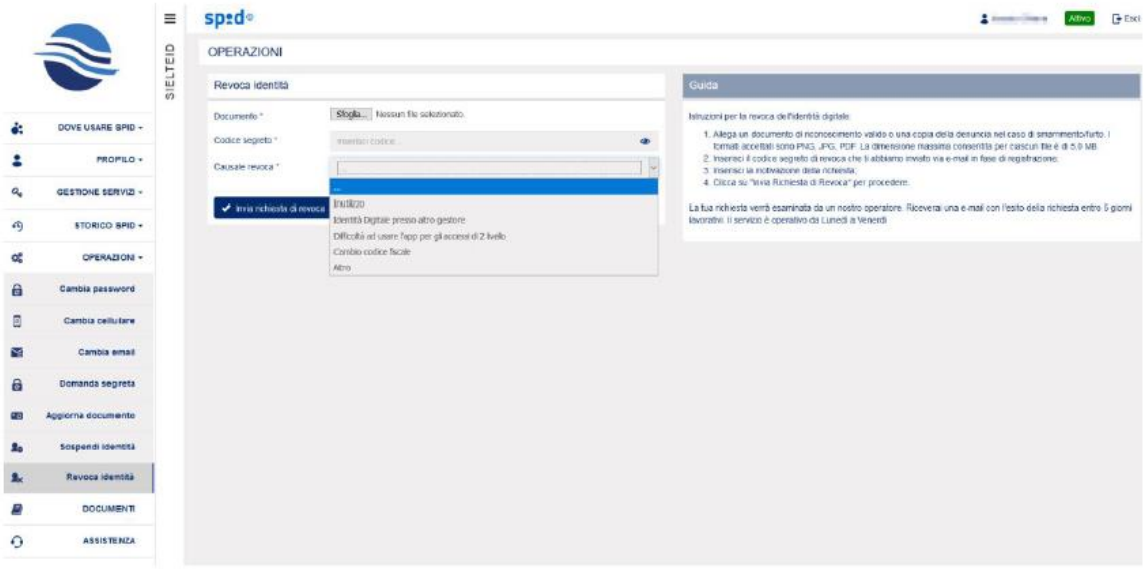


Figura 65 – Interfaccia di revoca dell’identità digitale

Il personale addetto di Sielte, che riceve le richieste di revoca, provvede a verificare tutta la documentazione ricevuta e l’eventuale validità della denuncia consegnata (solo nel caso di Furto e/o Smarrimento). Nel caso ci siano dei dati errati o la documentazione non sia valida, allora l’operatore provvede a contattare il cittadino al fine di individuare e correggere il problema.

Invece, nel caso in cui tutta la documentazione fornita per la revoca dell'identità digitale sia corretta, all'utente appare un messaggio di conferma di avvenuta revoca dell'identità digitale.

7.6 Rinnovo identità

L'utente riceverà per mail una comunicazione che gli ricorderà la data di scadenza della propria identità digitale. Al momento della scadenza, l'identità digitale gli verrà rinnovata per due anni in automatico e riceverà una mail di notifica.

L'utente può anche richiedere di non rinnovare automaticamente l'identità tramite una comunicazione da inviare all'indirizzo pec sistemi.sielte@legalmail.it. La comunicazione deve pervenire almeno trenta giorni prima, indicando la data a decorrere dalla quale si richiede la cessazione del servizio.

Qualora l'utente volesse usufruire nuovamente del servizio SPID, dopo il recesso, potrà effettuare una nuova registrazione per poi procedere all'identificazione.

7.7 Documenti

Cliccando su “Documenti”, dalla barra laterale, l’utente può accedere alla documentazione ufficiale di SielteID.

I documenti consultabili sono: “Condizioni generali”, “Manuale Utente”, “Manuale Operativo”, “Guida alla sicurezza dell’identità” e “Carta dei servizi”.

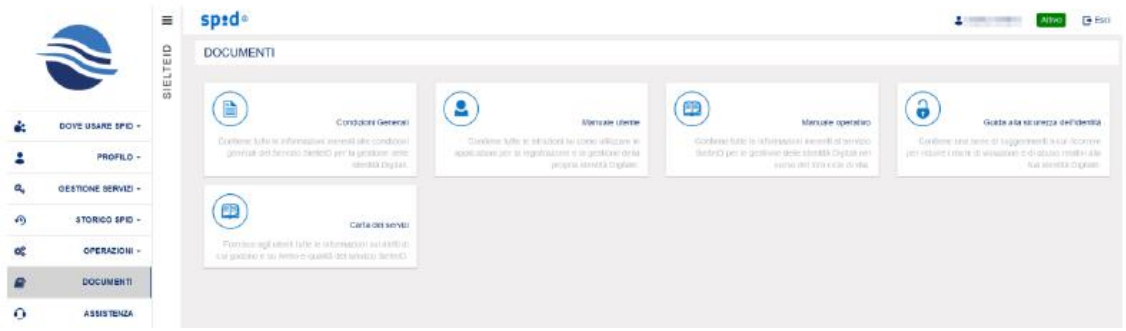


Figura 66 – Interfaccia con documentazione consultabile

7.8 Assistenza

Infine, cliccando su “Assistenza”, dalla barra laterale, l’utente può richiedere supporto per qualsiasi informazione grazie ad un Help Desk Sielte dedicato. Si può inviare anche un messaggio alla casella di posta spid@sielte.it per ottenere informazioni legate all’uso e al funzionamento dell’identità digitale.

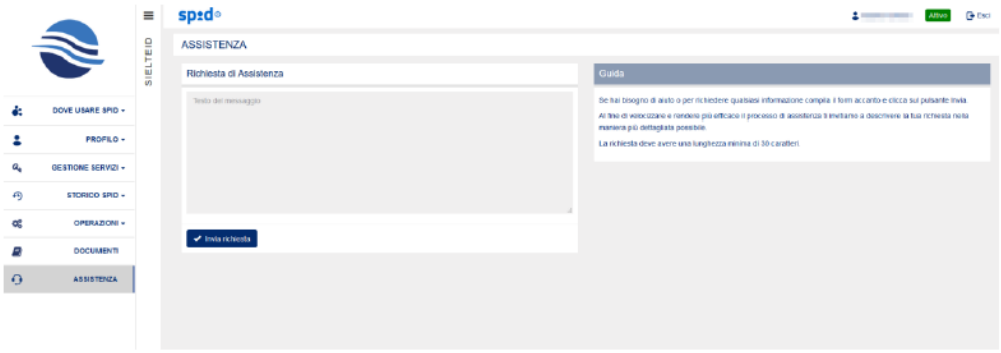


Figura 67 – Interfaccia di richiesta di assistenza

8 Autenticazione di livello 2

L'utente per accedere a determinati servizi della SPID della Pubblica Amministrazione e ad alcune operazioni del proprio profilo SielteID necessita di un'autenticazione di livello 2, inserendo nome utente e password ed un codice OTP.

Dalla pagina del proprio profilo SielteID, gli verrà richiesto l'accesso di Livello 2 come in Figura 68 – Interfaccia di richiesta accesso di Livello 2).

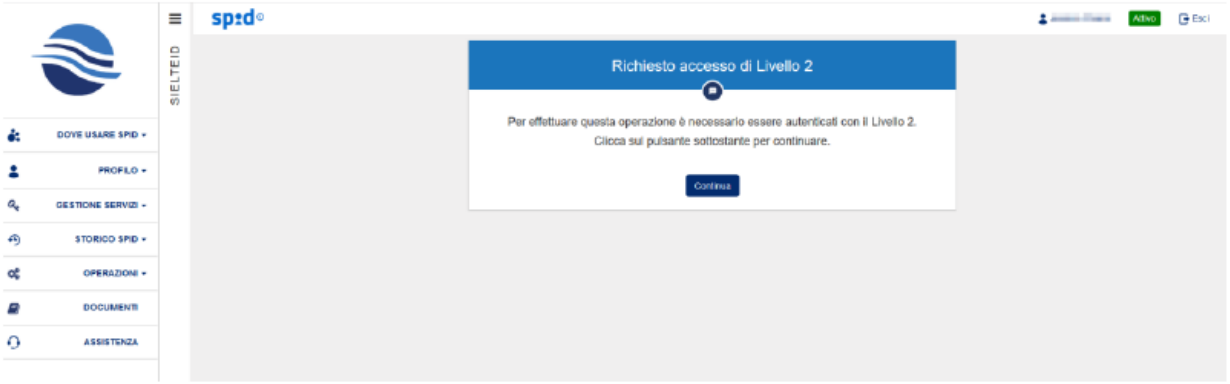


Figura 68 – Interfaccia di richiesta accesso di Livello 2

Gli utenti che hanno attivato l'applicazione MySielteID, ad ogni utilizzo che richieda di inserire le proprie credenziali SPID di Livello 2, possono utilizzare l'applicazione per generare il codice OTP o, nel caso di operazioni del profilo SielteID (vedi paragrafo 7.5) e qualora non avessero a disposizione un dispositivo su cui configurare l'applicazione, riceverlo via SMS tramite la voce "Richiedi OTP via sms". Altrimenti, possono accedere alle procedure di recupero, cliccando su "Ho perso il cellulare" o "Ho perso mail e cellulare", vedi capitolo 9.

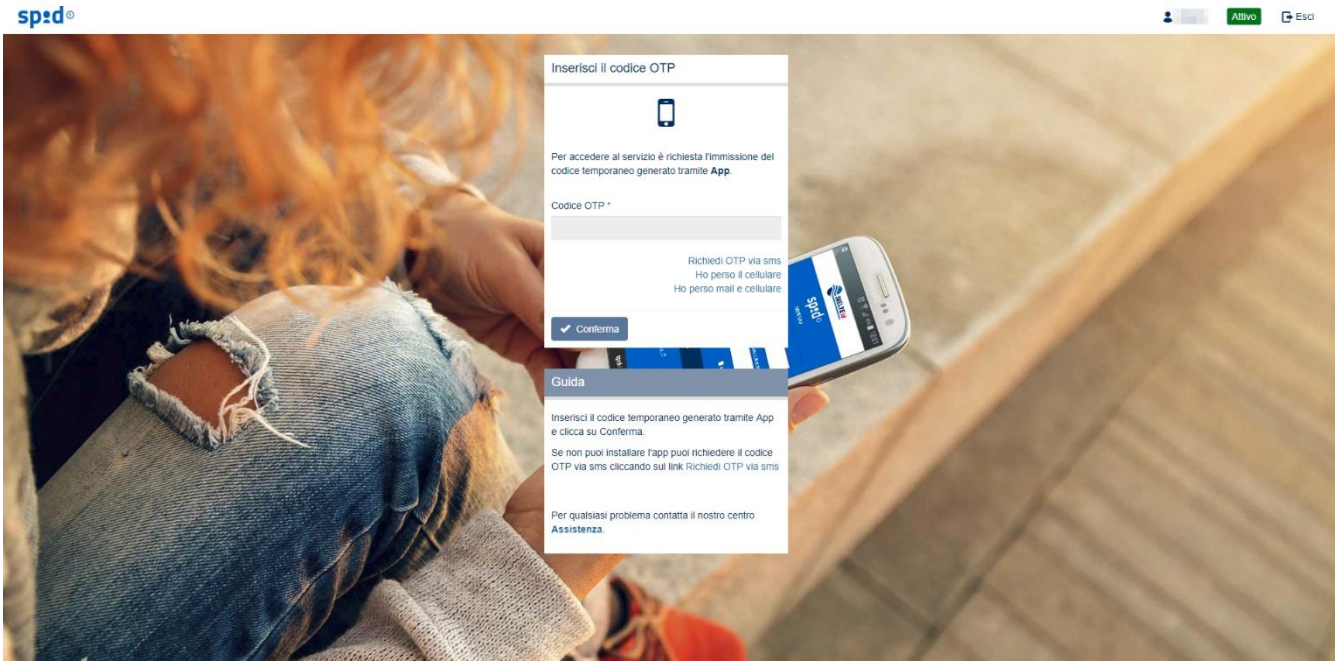


Figura 69 – Interfaccia di richiesta inserimento codice OTP

L'utente può verificare lo stato del proprio livello di autenticazione dall'icona SPID posta nella barra in alto a sinistra.

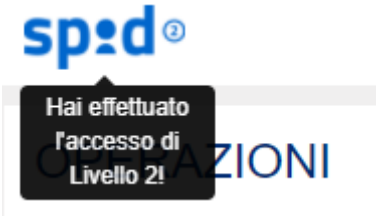


Figura 70 – Visualizzazione del livello di autenticazione

Dai servizi SPID viene avvisato di autenticarsi con il Livello 2 e di attivare le credenziali, qualora non fossero ancora attive, come in Figura 71 – Interfaccia di richiesta accesso di Livello 2 servizi SPID.

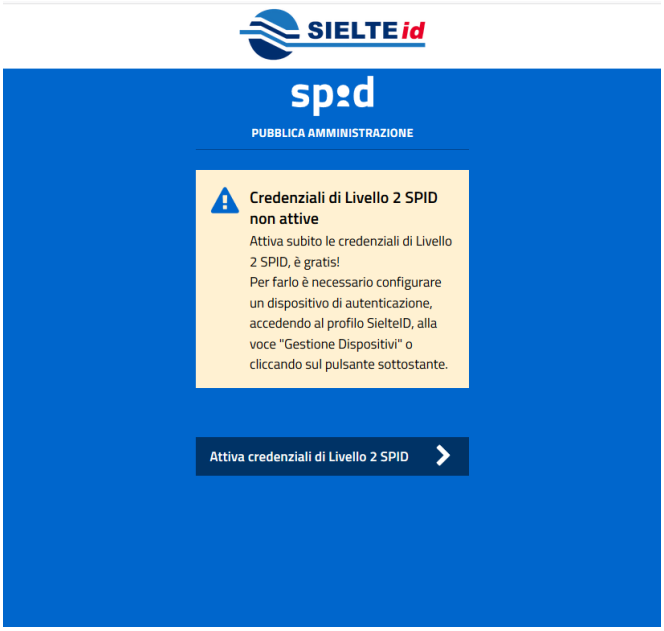


Figura 71 – Interfaccia di richiesta accesso di Livello 2 servizi SPID

9 Recupero delle credenziali

L'utente titolare di un'Identità Digitale ha la possibilità di poter recuperare le proprie credenziali di accesso al profilo SielteID, in base agli attributi in suo possesso.

9.1 Recupero password

Nel caso in cui l'utente abbia dimenticato la propria password di accesso e sia in possesso della mail e del cellulare associati alla sua identità SPID, può procedere al recupero tramite la voce **"Recupero password"**, presente nella login box di accesso.

Si avvia una procedura che permette all'utente di inserire il proprio Codice Fiscale e dichiarare che è in possesso sia del numero di cellulare che dell'indirizzo mail.

Figura 72 – Interfaccia di recupero password

Nel caso in cui sia ancora in possesso dell'indirizzo e-mail e del numero di cellulare, inseriti in fase di registrazione, l'utente riceve un codice OTP prima tramite e-mail, da inserire nel campo designato come nella figura sotto:

Figura 73- Interfaccia recupero password, verifica OTP via e-mail

Successivamente procede con la verifica del codice OTP via SMS, OTP da inserire nel campo designato come in figura sotto:

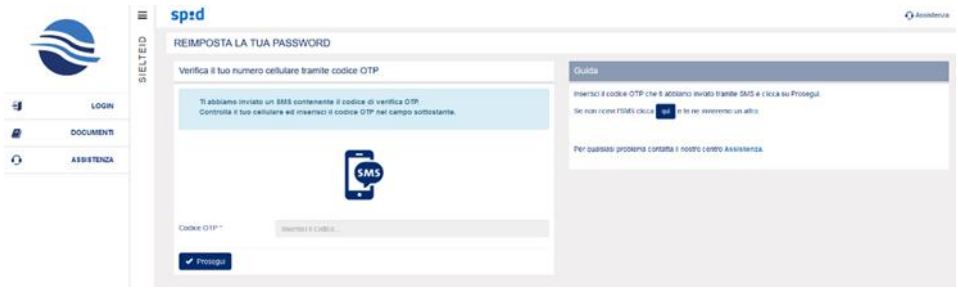


Figura 74- Interfaccia di recupero password, verifica OTP tramite SMS

A questo punto, verificati i due codici OTP, l'utente può procedere con il cambio password:

Figura 75- Interfaccia cambio password

9.2 Recupero password e cellulare

Nel caso in cui l'utente sia ancora in possesso dell'indirizzo e-mail, ma non del numero di cellulare associati alla sua identità SPID, gli verrà chiesto di rispondere ad un set di domande personali o alla domanda segreta precedentemente impostata.

Se la verifica andrà a buon fine, riceverà un codice OTP via e-mail.

Figura 76-Interfaccia di recupero password, in possesso solo di indirizzo email – verifica OTP

Validato quest'ultimo, potrà procederà all'inserimento di un nuovo numero di cellulare, sul quale ricevere un codice OTP, per far sì che venga verificato.

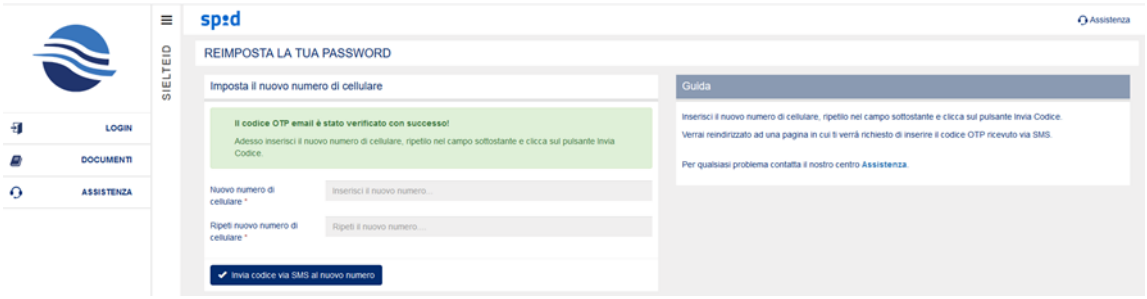


Figura 77-Interfaccia di recupero password, inserimento nuovo numero di cellulare

A questo punto, l'utente potrà procedere con il cambio password.

9.3 Recupero password ed e-mail

Nel caso in cui l'utente sia ancora in possesso del numero di cellulare, ma non dell'indirizzo e-mail associati alla propria identità SPID, gli verrà chiesto di rispondere ad un set di domande personali o alla domanda segreta precedentemente impostata.

Se la verifica andrà a buon fine, riceverà un codice OTP via SMS.

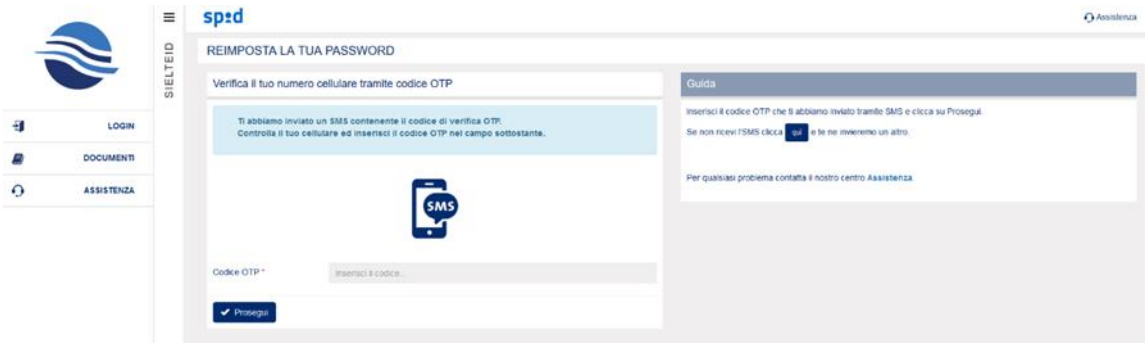


Figura 78- Interfaccia di recupero password, in possesso solo di numero di cellulare – verifica OTP

Validato quest'ultimo, potrà procedere all'inserimento di un nuovo indirizzo e-mail, sul quale riceverà un codice OTP, per far sì che venga verificato.

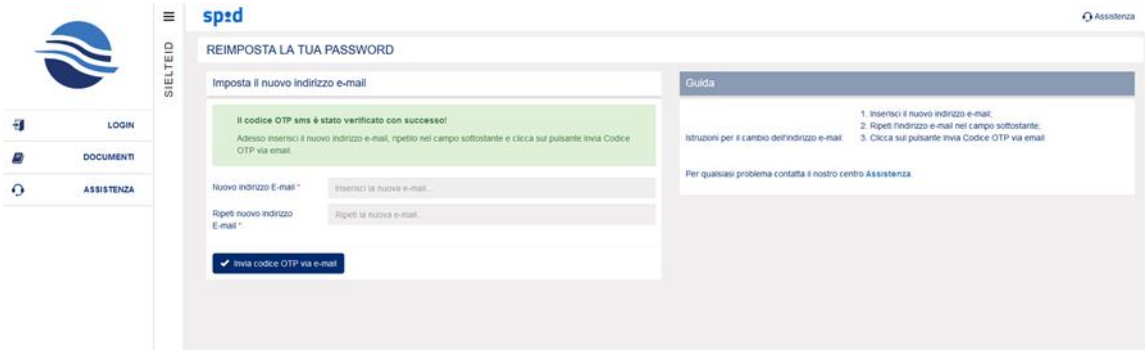


Figura 79- Interfaccia di recupero password, inserimento nuovo indirizzo e-mail

A questo punto, l'utente potrà procedere con il cambio password.

9.4 Recupero password, e-mail e cellulare

Nel caso in cui l'utente non sia in possesso, né dell'indirizzo e-mail, né del numero di cellulare, inseriti in fase di registrazione, per richiedere il cambio password dovrà rispondere ad una serie di domande personali quali:

- modalità di identificazione effettuata;

- numero di cellulare inserito in fase di registrazione;
- indirizzo mail inserito in fase di registrazione;
- tipo, numero e data di scadenza del documento di identità inserito in fase di registrazione;
- numero identificativo e data di scadenza della tessera sanitaria o numero identificativo del tesserino del codice fiscale nel caso di soggetti sprovvisti di tessera sanitaria, inserito in fase di registrazione;
- domanda segreta precedentemente impostata.

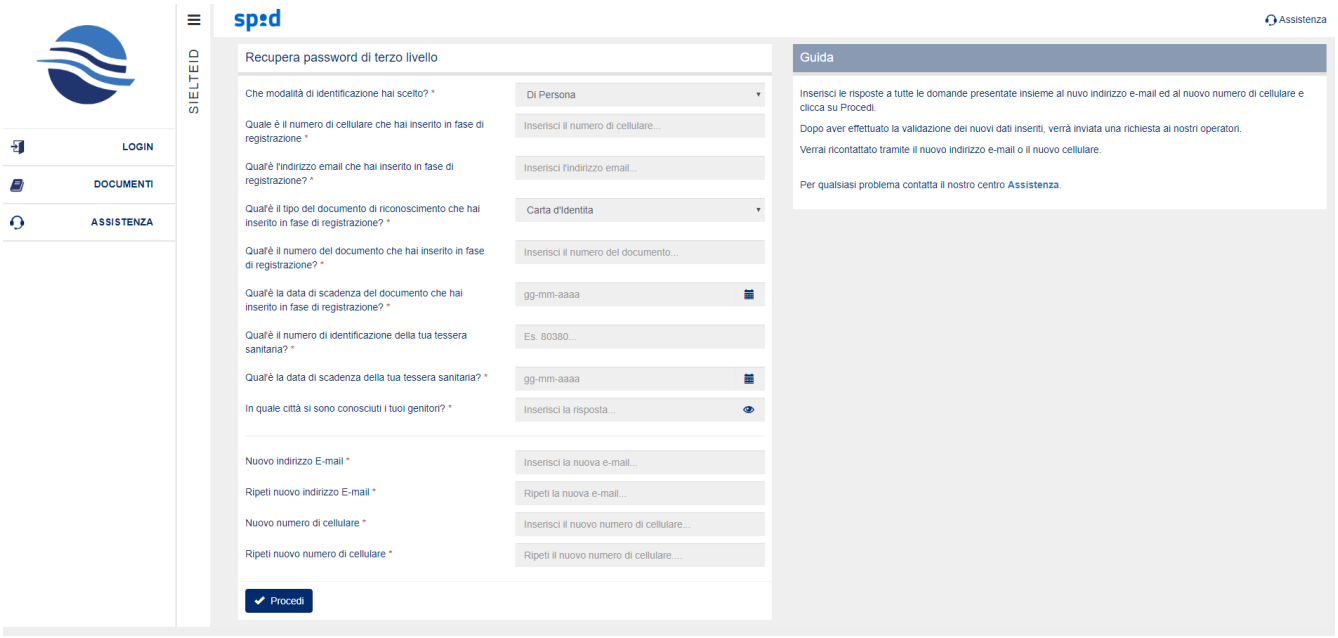


Figura 80- Form recupero credenziali

Successivamente dovrà inserire i nuovi indirizzo e-mail e numero di cellulare, sui quali riceverà un codice OTP da validare per la verifica.

A questo punto, validati i due codici, verrà inviata una *Richiesta di Recupero* agli operatori SielteID che la valuteranno. Se la richiesta viene approvata l'utente riceverà una mail con una

password temporanea con la quale potrà accedere al profilo e procedere all'inserimento di una nuova password.

Nel caso in cui l'operatore rigetti la *Richiesta di Recupero*, l'utente riceverà una mail in cui è specificato che la richiesta è stata respinta, di conseguenza dovrà ripetere la procedura, rispondendo correttamente a tutte le domande. L'operatore al terzo tentativo rigettato sospende l'identità per motivi di sicurezza.

Nel caso in cui l'utente nella richiesta di recupero non soddisfi i requisiti utili per effettuare il recupero delle credenziali dovrà provvedere ad inviare una richiesta di revoca tramite pec all'indirizzo sistemi.sielte@legalmail.it allegando, oltre alla richiesta, copia dei documenti di riconoscimento. Qualora l'utente volesse usufruire del servizio SPID, dopo la revoca, potrà effettuare una nuova registrazione per procedere all'identificazione.

10 Recupero codici dispositivi

Nel caso in cui l'utente non è in possesso dei codici dispositivi, per effettuare alcune delle operazioni di cui sopra sull'identità digitale, può richiederne la sostituzione contattando il supporto di Sielte che provvederà a fornire via e-mail i nuovi codici.

11 Supporto dedicato

Sielte mette a disposizione dei propri utenti un servizio di Service Desk affidabile ed efficiente che rende molto più semplice il processo di richiesta assistenza e gli scambi di informazioni tra utenti e operatori.

Questo servizio può essere utilizzato attraverso due canali di comunicazione:

- E-mail: inviando una mail all'indirizzo di posta spid@sielte.it la quale deve contenere la descrizione, il più dettagliata possibile, del problema riscontrato.

- Telefono: l'utente può richiedere informazioni o assistenza tramite il seguente Numero 095 7171301, con operatore disponibile dal lunedì al sabato, dalle ore 09:00 alle ore 18:00.