Namirial ID

SPID – Guida utente

Categoria	**SPID**	Codice Documento	**NAM-SPID-GU**	**Namirial S.p.A.**
Redatto da	**Luca Pernini**	Nota di riservatezza	**Documento Pubblico**	Il Legale Rappresentante
Verificato da	**Simone Baldini**	Versione	**1.4**	**Enrico Giacomelli**
Approvato da	**Enrico Giacomelli**	Data di emissione	**25/03/2020**	GIACOMELLI EN 2020.03.26 20:45:58 CN=GIACOMELLI ENRICC C=IT 2.5.4.4=GIACOMELLI 2.5.4.42=ENRICO RSA/2048 bits

Namirial S.p.A.

Sede legale, direzione e amministrazione 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
C.F./ISCR. REG. IMPR. ANCONA N.02046570426 - P.I. IT02046570426 - CAP. SOC. € 6.500.000,00 i.v.
Tel. 07163494 s.a. - Fax 199.418016 - info@namirialtsp.com - www.namirial.com

– Questa pagina è lasciata intenzionalmente in bianco –

INDICE

STORIA DELLE MODIFICHE APPORTATE

VERSIONE	1.4
Data	25/03/2020
Motivazione	Aggiornamento e revisione annuale.
Modifiche	RIFERIMENTI: aggiornato riferimento al Regolamento GDPR Aggiornato il manuale con i nuovi riferimenti grafici al Portale che il Gestore ha appositamente predisposto per la Richiesta e Gestione di un'identità digitale. Inserita la descrizione della procedura per il video riconoscimento. Corretti refusi di digitazione

VERSIONE	1.3
Data	04/07/2017
Motivazione	Quarta emissione del documento.
Modifiche	Aggiornato nome servizio SPID Aggiornati link siti web e indirizzi e-mail

VERSIONE	1.2
Data	08/05/2017
Motivazione	Terza emissione del documento.
Modifiche	Inserito obbligo upload Tessera Sanitaria Dettagliata l'accettazione dei consensi Rimosso logo eIDAS dalle pagine dell'IDP Precisata la durata della password Dettagliati i livelli di sicurezza per l'accesso alle funzioni di revoca, sospensione e gestione dell'Identità Specificata la possibilità di richiedere la revoca o sospensione con firma elettronica Specificata la possibilità di inviare anche comunicazioni al Gestore

VERSIONE	1.1
Data	30/03/2017
Motivazione	Sec onda emissione del documento.
Modifiche	Inserito riconoscimento con Firma Digitale, CNS, TS/CNS e CIE Inserito il supporto per token OTP hardware OATH compliant

VERSIONE	**1.0**
Data	01/03/2017
Motivazione	Prima emissione del documento.
Modifiche	---

RIFERIMENTI

NUMERO	DESCRIZIONE
[I]	Decreto del Presidente della Repubblica (DPR) 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.
[II]	Decreto del Presidente del Consiglio (DPCM) 24 ottobre 2014 "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché d ei tempi e delle modalità di azione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese", pubblicato sulla Gazzetta Ufficiale del 9 dicembre 2014, n.285
[III]	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE)
[IV]	Decreto Legislativo (CAD) 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale", pubblicato nella Gazzetta Ufficiale n.112 del 16 maggio 2005 con le modifiche ed integrazioni stabilite dal decreto legislativo 26 agosto 2016, n. 179.
[V]	Decreto Legislativo (DLGS 69) 21 giugno 2013, n. 69, convertito con modificazioni dalla legge del 9 agosto 2013, n. 69 che "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese".
[VI]	Regolamento UE n.910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, pubblicato nella Gazzetta Ufficiale dell'Unione Europea – serie L 257 del 28 agosto 2014.
[VII]	Regolamento recante le regole tecniche (articolo 4, comma 2, DPCM 24 ottobre 2014) per il gestore dell'identità digitale.
[VIII]	Regolamento recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014)
[IX]	Regolamento recante le modalità per l'accreditamento e la vigilanza dei Gestori dell'Identità digitale (articolo 1, comma 1, lettera l) , DPCM 24 ottobre 2014).
[X]	Determinazione AgID n.16/2016: Pubblicazione di "Avvisi" sulle procedure tecniche inerenti il Sistema Pubblico per la gestione dell'Identità digitale (SPID) sul portale istituzionale dell'Agenzia.
[XI]	AgID – SPID: Note tecniche sulle interfacce e sulle informazioni IdP/SP.
[XII]	ISO EN UNI 9001:2015 – Sistema Qualità
[XIII]	ISO/IEC 29115:2013 Information technology - Security techniques - Entity authentication assurance framework
[XIV]	Regolamento UE n.1502/2015 della Commissione dell'8 settembre 2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
[XV]	ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

Tabella 1: - Riferimenti normativi

INDICE DELLE TABELLE

INDICE DELLE FIGURE

1 INTRODUZIONE

1.1 SCOPO DEL DOCUMENTO E CAMPO DI APPLICAZIONE

Il presente documento, identificato mediante il codice riportato nel frontespizio, descrive le modalità per la richiesta ed uso del servizio di autenticazione SPID, le modalità con cui l'utente può richiedere la sospensione o la revoca delle credenziali non ché le cautele che l'utente deve adottare per la conservazione e la protezione delle credenziali SPID.
Più in dettaglio descrive l'interazione tra l'utente e il Gestore Namirial S.p.A. nell'ambito del suo ruolo di IDP per l'erogazione del servizio SPID per quanto concerne:

1. Richiesta credenziale SPID;
2. Registrazione, validazione e verifica dei dati forniti;
3. Rilascio della credenziale SPID;
4. Utilizzo e custodia delle credenziali SPID;
5. Sospensione e Revoca della credenziale SPID;
6. Variazione dei dati della credenziale;
7. Scadenza e Rinnovo della credenziale.

SPID (Sistema Pubblico per l'Identità Digitale) nasce per garantire a tutti i cittadini ed alle imprese un accesso unico, sicuro e protetto ai servizi digitali proposti dalla Pubblica Amministrazione e dai soggetti privati aderenti.
Rappresenta il passo successivo verso l'autenticazione e l'identificazione sicura: l'idea di fornire ai cittadini ed alle imprese un'unica identità digitale per accedere online a molteplici servizi sia privati che pubblici eliminando la necessità di dover utilizzare profili e password sempre diversi. La sicurezza è garantita poiché il rilascio e la gestione dell'Identità SPID e dei suoi attributi qualificati possono essere effettuati unicamente da soggetti accreditati da AgID.

I soggetti coinvolti nei processi SPID sono:

1. IDP – Identity Provider o Gestore dell'Identità Digitale: soggetto accreditato da AgID con finalità di creazione e gestione delle identità.
2. SP – Service Provider o Fornitore di servizi: soggetto, sia pubblico che privato, che eroga dei servizi tramite propri siti internet utilizzando come modalità di accesso le credenziali SPID.
3. Utente: soggetto fruitore dei servizi, titolare di un'identità SPID.

1.2 DEFINIZIONI ED ACRONIMI

Sono di seguito elencati i termini, gli acronimi e le definizioni utilizzati nella stesura della presente Guida Utente. Per i termini definiti dal CAD e dal DPCM si rimanda alle definizioni in essi contenute. Dove appropriato viene indicato anche il termine inglese corrispondente, generalmente usato in letteratura tecnica e negli standard.

TERMINE	SIGNIFICATO
AA	Attribute Authority
Adesione	E' il recepimento del framework SPID da parte di entità di certificazione o di fornitori di servizi in rete.
Agenzia (anche AgID)	Agenzia per l'Italia Digitale (anche Autorità di Accreditamento e Vigilanza sui Gestori di Identità Digitali)
Analisi dei rischi	Processo di comprensione della natura del rischio e di determinazione del livello di rischio.
Attributi identificativi	Nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, il codice fiscale o la partita IVA e gli estremi del documento d'identità utilizzato ai fini dell'identificazione;
Attributi secondari	Il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni
Autenticazione multi-fattore	Autenticazione con almeno due fattori di autenticazione indipendenti (ISO-IEC 19790)
Autenticazione	Disposizione di garanzia sull'identità dell'entità (ISO-IEC 18014-2)
Autorizzazione	Processo volto ad accertare che l'informazione sia accessibile esclusivamente a coloro che sono autorizzati all'accesso.
CA	Certification Authority
Codice identificativo	Il particolare attributo assegnato dal gestore dell'identità' digitale che consente di individuare univocamente un'identità digitale nell'ambito dello SPID
Credenziale	Un insieme di dati presentati come evidenza dell'identità dichiarata/asserita o di un proprio diritto (ITU-T X.1252), in pratica il Titolare/utente si avvale di questo attributo (a singolo o doppio fattore) unitamente al codice identificativo (entrambi rilasciati dal gestore dell'identità digitale) per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi (Amministrazioni e privati) che aderiscono allo SPID
Criteri di rischio	Valori di riferimento rispetto ai quali è ponderato il rischio.
Dato Personale	Si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4, com. 1) del [III]).
Dati Particolari	Sono quei "dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (art. 9 .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. 9, com. 1) [III]).
Dati giudiziari	Vedi Dati Particolari
Disponibilità	Accertarsi che gli utenti autorizzati abbiano accesso all'informazione e alle attività associate quando richiesto.
Definizione del rischio	Processo di individuazione, riconoscimento e descrizione del rischio.
EAA	Entity Authentication Assurance
Entità	Può essere una persona fisica o un soggetto giuridico
ETSI	European Telecommunications Standards Institute
Fattore di autenticazione	Elemento di informazione e/o processo usato per autenticare o verificare l'identità di una entità (ISO-IEC 19790)
Fornitore di servizi	Il fornitore dei servizi della società dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al gestore dell'identità digitale che l'ha fornita
Gestione del rischio	Attività coordinate per dirigere e controllare una organizzazione in merito al rischio o ai rischi esistenti.
Gestori dell'identità digitale	Le persone giuridiche accreditate allo SPID che, in qualità di gestori di servizio pubblico, previa identificazione certa dell'utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Essi inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti.
Gestori di attributi qualificati	I soggetti accreditati ai sensi dell'art. 16 del DPCM 24 ottobre 2014 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.
Identità digitale	La rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale.
IDM	Identity Management
IDP	Identity Provider (il gestore delle identità digitali in ambito SPID)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPV	Identity Proofing and Verification
IS	International Standard
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
Integrità	Salvaguardia dell'esattezza e della completezza dei dati e delle modalità di processo.
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector

LoA	Level of Assurance
NIST	National Institute of Standards and Technology
RAO	Operatore o Incaricato del Gestore al riconoscimento del soggetto richiedente l'identità SPID
OTP	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione
PII	Personally Identifiable Information
Ponderazione del rischio	Processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio è accettabile o tollerabile.
Riservatezza	Garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate
SAML	Security Assertion Markup Language
SSL	Secure Socket Layer
SP	Service provider – vedi Fornitore Servizi
SPID	Il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98
TCP	Transmission Control Protocol
Titolare	E' il soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SPID, corrisponde all'utente del DPCM art. 1 comma 1 lettera v)
Trattamento del rischio	Processi di selezione e implementazione di attività volte a diminuire o comunque modificare il rischio presente.
User Agent	Sistema utilizzato dall'utente per l'accesso ai servizi (di solito il browser per la navigazione in rete);
Valutazione del rischio	Processo complessivo di identificazione, analisi e ponderazione del rischio.

Tabella 2: - Definizioni ed Acronimi

2 RICHIESTA E RILASCIO DEL SERVIZIO SPID

La richiesta, ed il successivo rilascio delle credenziali SPID, avviene tramite una procedura web-based, articolata in diverse macro-fasi atte a mappare i principali passaggi previsti dalle regole attuative, ovvero:

Fase	Regole Attuative
• Scelta della tipologia di identità: soggetto fisico / soggetto giuridico	Richiesta/Registrazione
• Inserimento degli attributi secondari (Username, E-mail, Cellulare) • Inserimento dati anagrafici	Registrazione/Identificazione
• Acquisizione Documento di Identità e Tessera Sanitaria, entrambi in corso di validità, e adeguata verifica	Identificazione/Verifica dell'Identità dichiarata
• Esplicito consenso alla richiesta di attivazione dell'identità • Verifica dell'identità con riconoscimento a vista (a sportello) o con identificazione informatica (CNS, CIE, Firma Digitale) • Scelta livello e tipo di credenziali	Identificazione
• Attivazione Identità e Credenziali • Verifica attributi secondari	Verifica/Emissione dell'Identità
• Completamento e consegna delle Credenziali	Consegna credenziali

Tabella 3 - Fasi procedura rilascio identità SPID

2.1 REGISTRAZIONE DATI DELL'UTENTE (RICHIESTA ONLINE)

La registrazione online dell'identità SPID si sviluppa attraverso un processo guidato che accomuna la fase di registrazione con quella di identificazione. Per poter completare la registrazione è necessario che l'utente abbia con sé, oltre ai dati anagrafici, un numero di telefonia mobile (necessario per ricevere le comunicazioni SMS), una casella e-mail attiva, un documento di identità e la Tessera Sanitaria, entrambi in corso di validità. In alcuni casi particolari potrebbe essere necessario che l'utente si debba recare presso le LRA di Namirial S.p.A. per l'attivazione delle credenziali di accesso.
Il link per procedere con la richiesta della identità digitale è il seguente: https://portal.namirialtsp.com/.
Cliccando il bottone "Registrati", si avvia la procedura di registrazione dei dati così come descritta nei seguenti paragrafi.

2.1.1 REQUISITI

Per procedere alla richiesta di attivazione tramite procedura web-based, è necessario che la postazione utilizzata rispetti i seguenti requisiti:

Sistema Operativo:

- Da Windows 7
- Da Windows Server 2008 R2 (quindi esclusi XP e Vista)
- Da OS X 10.9

Browser:

- Da Internet Explorer 11+
- Da Microsoft EDGE 25+
- Da Chrome 30+
- Da Firefox 27+
- Da Opera 17+

Protocolli:

- http e https, porte 80, 443, 8080

2.1.2 ACCETTAZIONE E CONSENSI

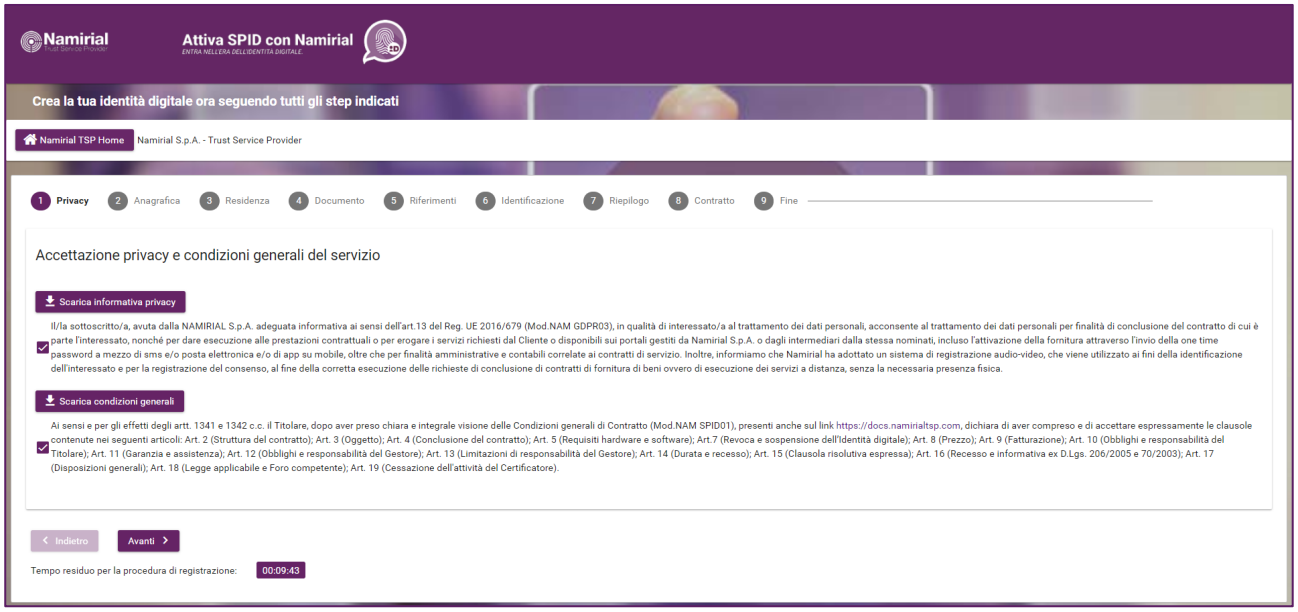
La fase di "Accettazione e Consensi" è suddivisa in due sezioni:

1. Clausole di accettazione per l'ottenimento dell'Identità Digitale SPID (accettazione obbligatoria)
2. Altre clausole di natura commerciale e di marketing (accettazione facoltativa)

La sezione 1 prevede l'indicazione di accettazione delle condizioni di utilizzo e privacy e raccolta del consenso all'adesione al servizio. In questa sezione vengono fornite opportune notifiche riguardo:

- Consenso privacy – apporre un segno di spunta nel campo per passare allo stato "Accetto"
- Termini e condizioni – apporre un segno di spunta nel campo per passare allo stato "Accetto"

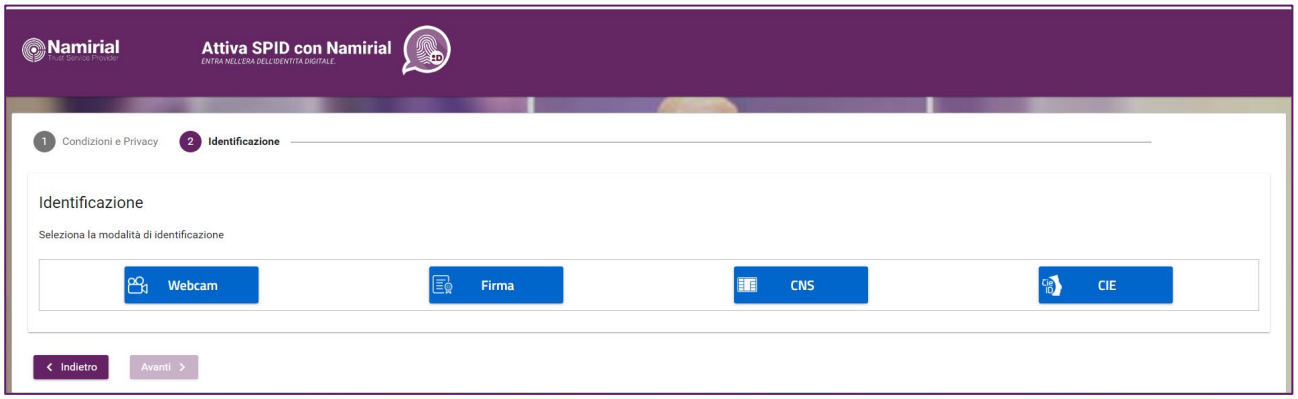
La sezione 2 prevede la possibilità di usufruire di servizi aggiuntivi che prevedono l'accettazione di ulteriori condizioni di natura commerciale e marketing.



2.1.3 MODALITÀ' DI IDENTIFICAZIONE

All'interno di questa funzione è possibile indicare la modalità prescelta per eseguire l'identificazione certa del richiedente:

a. **Riconoscimento tramite TS-CNS, CNS, CIE**
   Utilizzando la propria CIE (Carta di Identità Elettronica) o CNS (Carta Nazionale dei Servizi), può procedere alla convalida della richiesta scaricando il modulo di adesione SPID precompilato, sottoscriverlo elettronicamente con la propria CIE o CNS e caricarlo nelle pagine in modo da convalidare automaticamente la richiesta di attivazione.
b. **Firma Digitale**
   L'utente in possesso di un certificato di firma digitale valido può scaricare il modulo di adesione SPID precompilato, sottoscriverlo digitalmente con gli strumenti normalmente usati, e caricarlo nelle pagine in modo da convalidare automaticamente la richiesta di attivazione.
c. **Web Cam**
   L'utente in possesso di un dispositivo desktop, portatile o mobile dotato di webcam e microfono, può effettuare il riconoscimento audio video attraverso una procedura conforme all'Art 8 del Regolamento recante modalità attuative per la realizzazione dello SPID

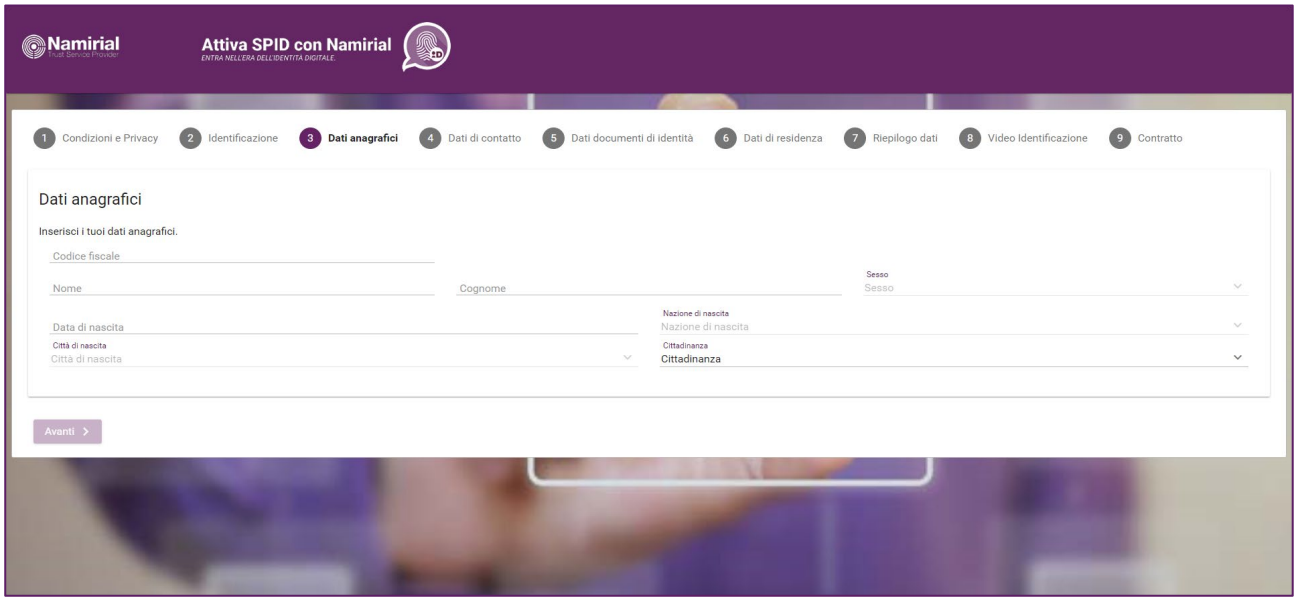


2.1.4 ANAGRAFICA

La fase, "**Anagrafica**", è destinata all'inserimento delle seguenti informazioni e si svolge in due passaggi:

Passo1 - vengono richiesti i dati anagrafici:

- **Codice Fiscale** – inserire il codice fiscale
- **Nome** – inserire il nome del registrante
- **Cognome** – inserire il cognome del registrante
- **Sesso** – inserire il sesso Maschio / Femmina
- **Data di nascita** – inserire la data di nascita nel formato gg/mm/aaaa
- **Nazione di nascita** – valore data di nascita
- **Comune di nascita** – indicare il comune di nascita



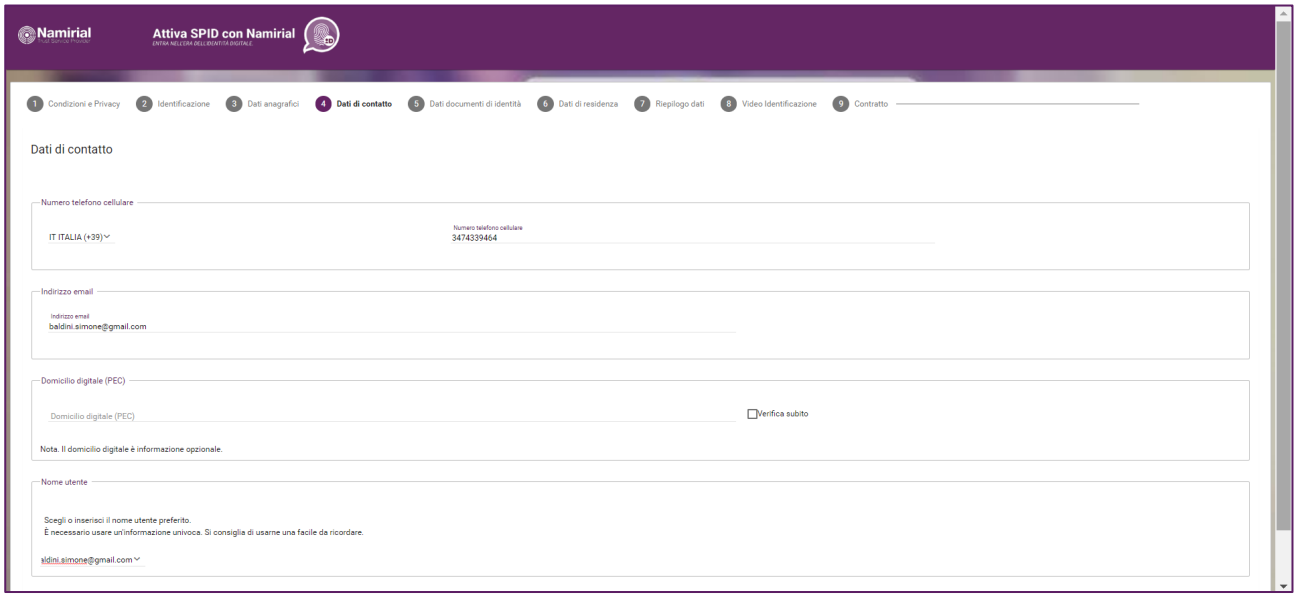
2.1.5 ATTRIBUTI SECONDARI: NUMERO TELEFONICO E INDIRIZZO E-MAIL

Questa fase richiede la registrazione dell'**indirizzo email** e **numero di cellulare**

Email: prevede la registrazione della casella email del Titolare per l'accesso ai **servizi SPID**. Questa informazione verrà censita come attributo secondario.

Cellulare: prevede la registrazione del numero di telefono del Titolare per l'accesso ai **servizi SPID**. Questa informazione verrà censita come attributo secondario.

Il possesso dell'email e del cellulare sono verificati durante la fase di registrazione. Il numero di telefono, tramite apposita opzione, è verificato mediante l'invio di un codice via SMS al numero indicato. Per la verifica dell'indirizzo di posta elettronica, il sistema invia allo stesso indirizzo un codice di verifica.
I codici inviati via SMS e via email devono essere reinseriti in procedura, all'interno degli appositi campi, al fine di completare la verifica e procedere nel flusso.

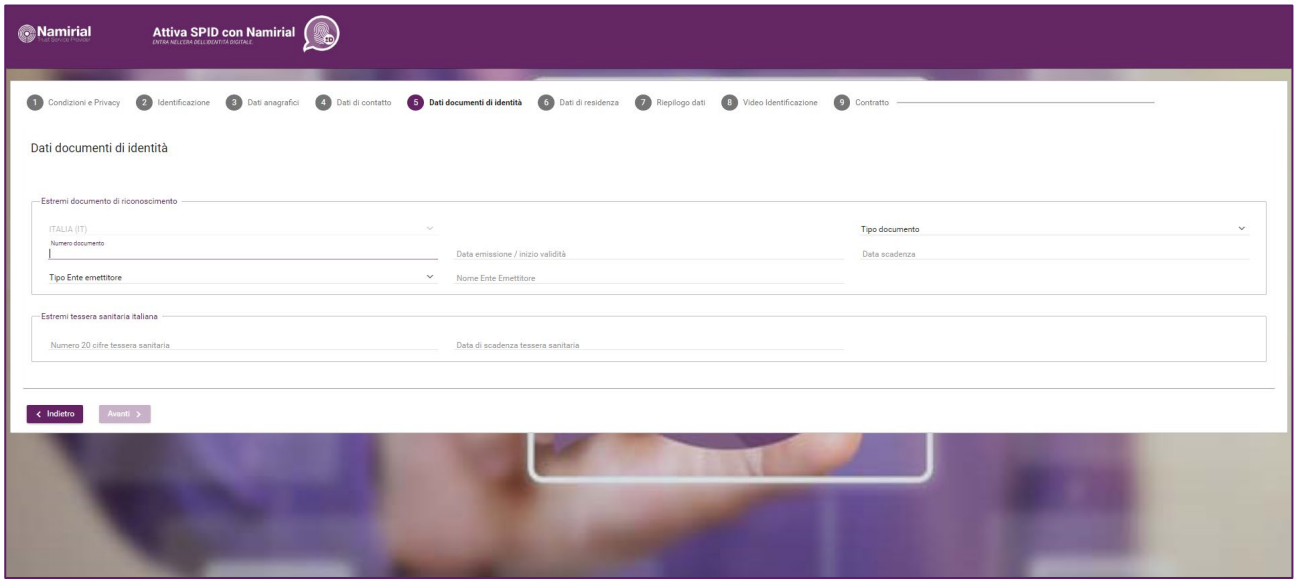


In questa fase l'utente può scegliere anche lo username che verrà utilizzato per l'identità digitale.

2.1.6 DOCUMENTO

La fase "**Documento**" prevede la registrazione delle seguenti informazioni:

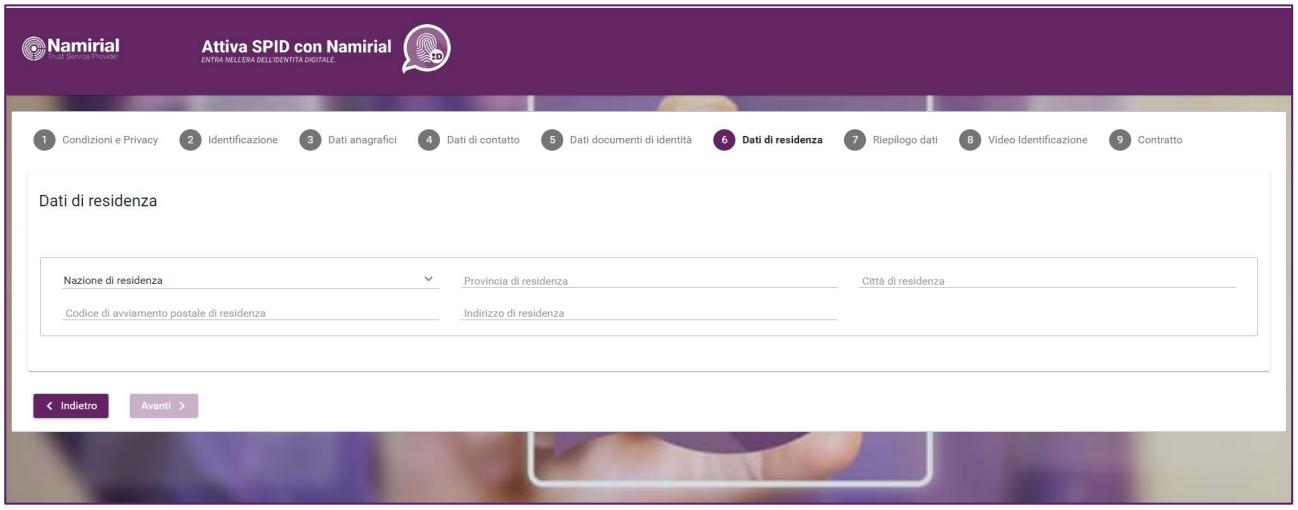
- **Tipo documento** – indicare la tipologia di documento che si intende utilizzare per la registrazione, tra le possibili voci (Carta di Identità, Patente di Guida, Passaporto,)
- **Numero documento** – inserire il numero del documento utilizzato per la registrazione
- **Data di emissione** – inserire la data di emissione del documento nel formato gg/mm/aaaa
- **Data di scadenza** – inserire la data di scadenza del documento nel formato gg/mm/aaaa
- **Tipologia dell'Ente che ha emesso il documento** – inserire "Comune" per Carta di Identità, etc etc…
- **Ente emittente** – inserire il nome dell'ente che ha emesso il documento



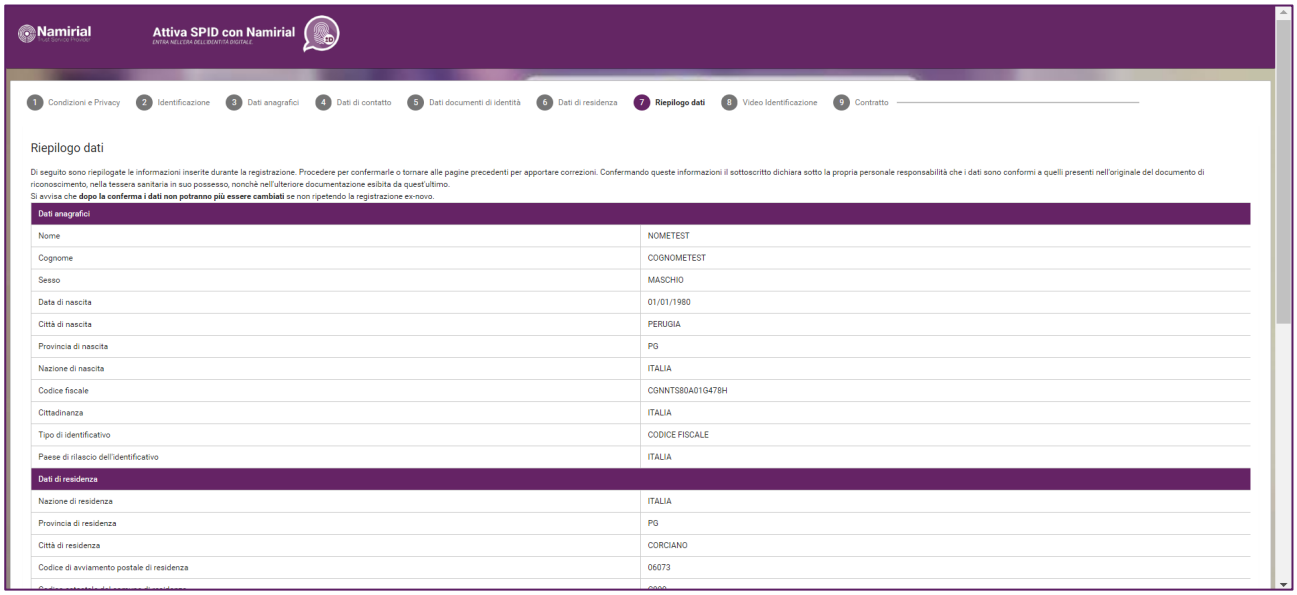
2.1.7 RESIDENZA

La fase "**Residenza**" prevede la registrazione delle seguenti informazioni:

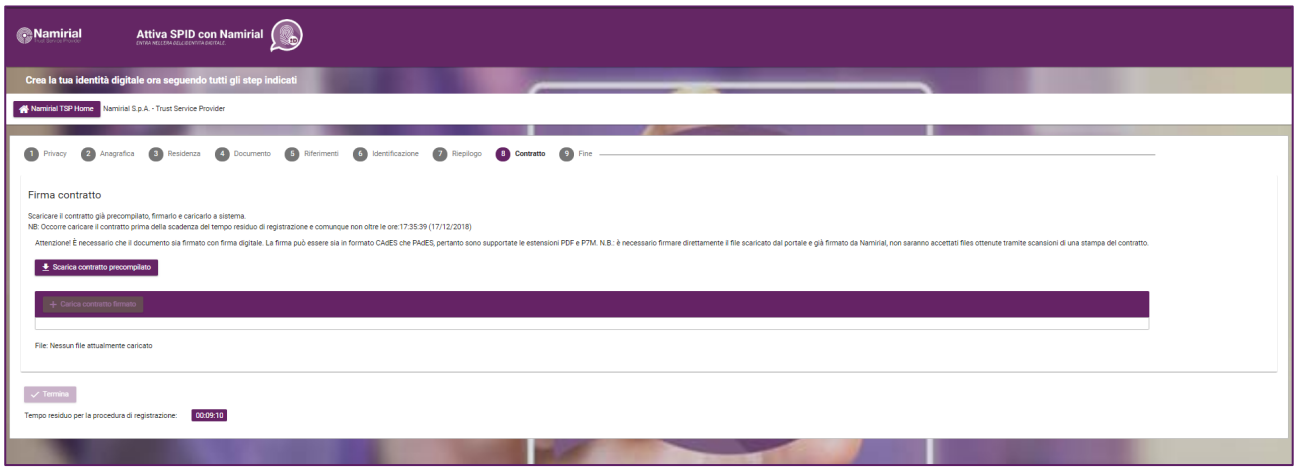
- **Nazionalità** – indicare la nazionalità
- **Comune di residenza** – inserire il proprio comune di residenza
- **Provincia di residenza** – indicare la provincia di residenza
- **CAP** – valore del CAP del comune di residenza
- **Indirizzo di residenza** – comprensivo del numero civico



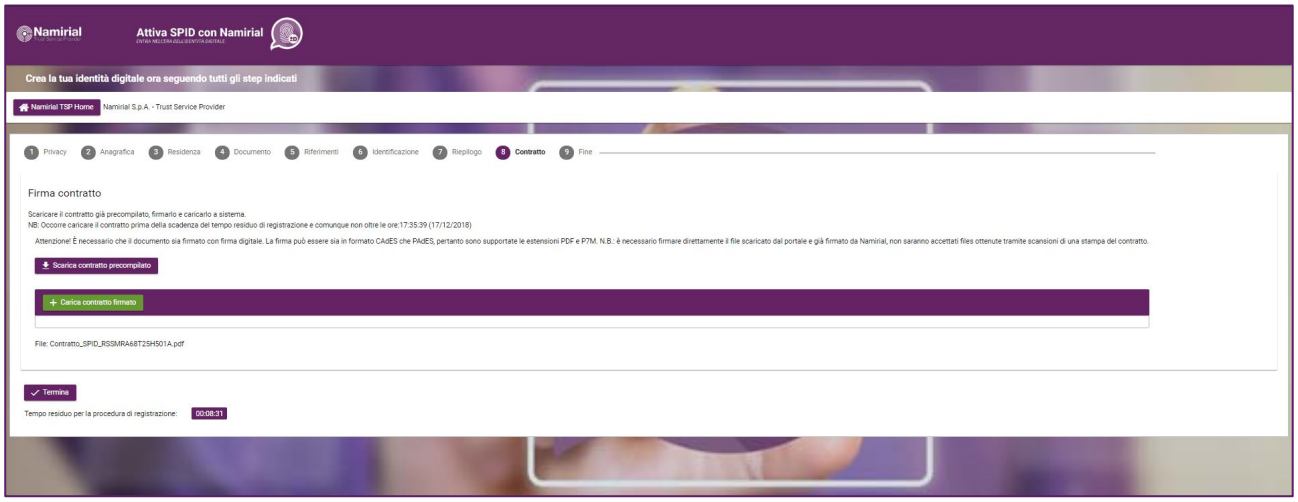
Terminata la fase di inserimento dati di identificazione viene presentato il riepilogo dei dati inseriti:



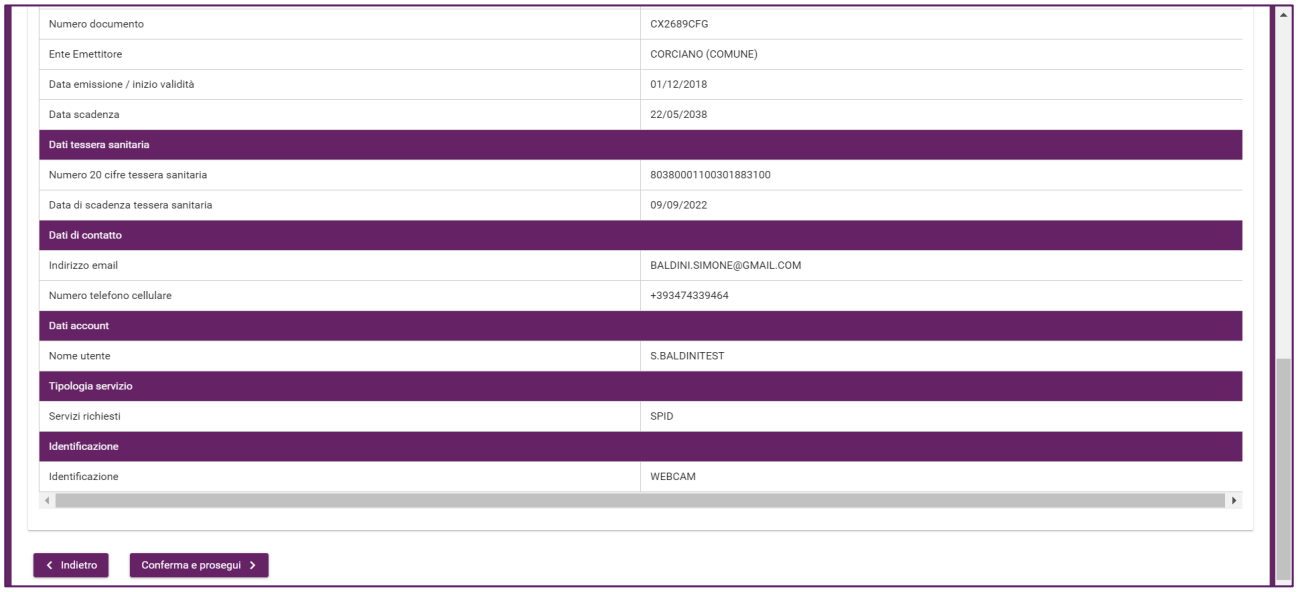
Nei casi in cui il Richiedente non abbia optato per il riconoscimento tramite firma digitale la procedura prosegue con la firma del contratto secondo quanto riportato nella schermata seguente.



Una volta firmato digitalmente il contratto, è possibile caricarlo utilizzando l'apposita funzione come mostrato dalla schermata seguente:

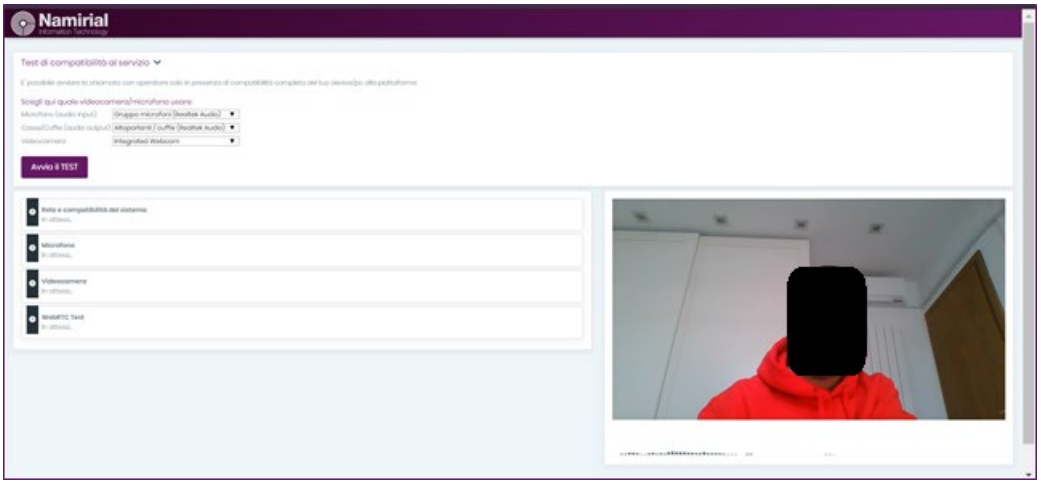


Nel caso in cui l'utente abbia richiesto l'identificazione via WebCam viene avviato il processo descritto nelle figure che seguono:

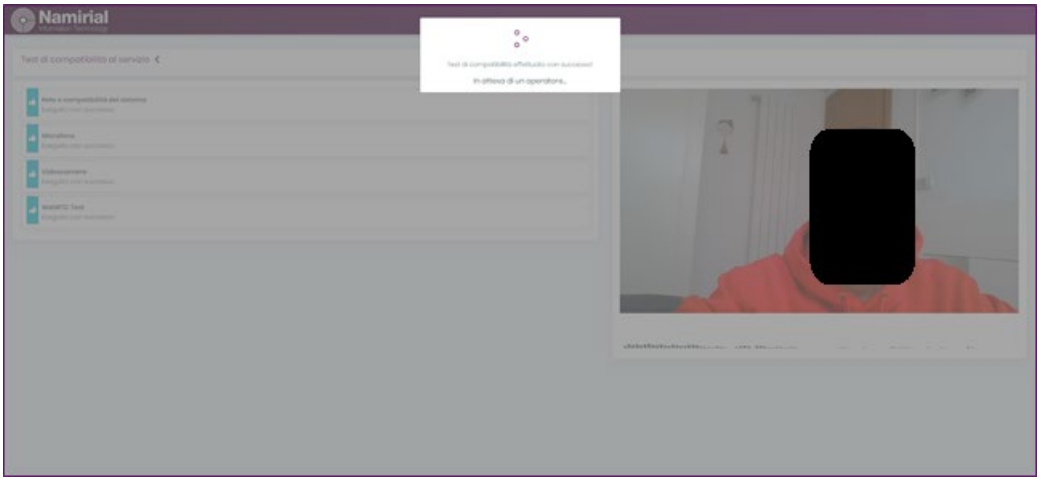


L'utente avvia il videoriconoscimento

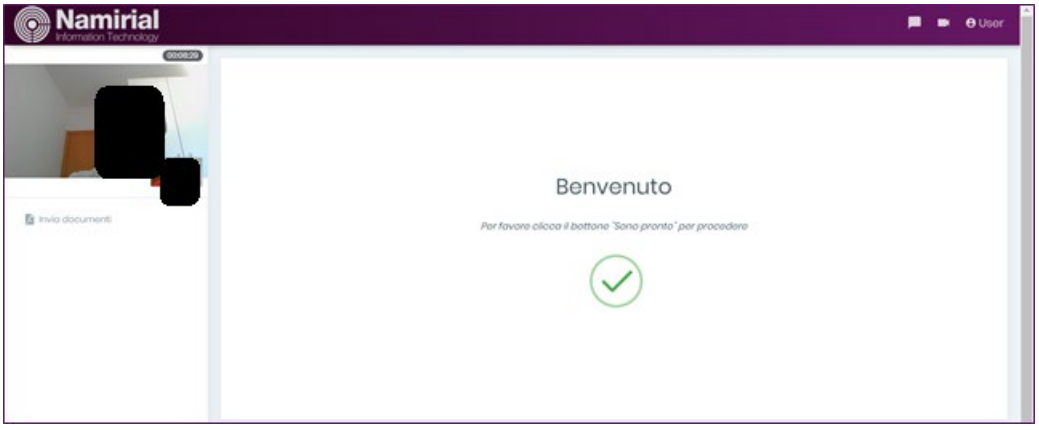
Step 1 - Verificare la compatibilità del microfono e della webcam:
L'identificazione via webcam avviene con strumenti audio/video quindi è indispensabile utilizzare un microfono e una webcam funzionanti. Pertanto, il sistema verifica la compatibilità degli strumenti e della configurazione della postazione



Step 2- Una volta completata la fase di verifica della strumentazione e della configurazione dell'utente, viene effettuata la chiamata in attesa di un operatore di riconoscimento libero.

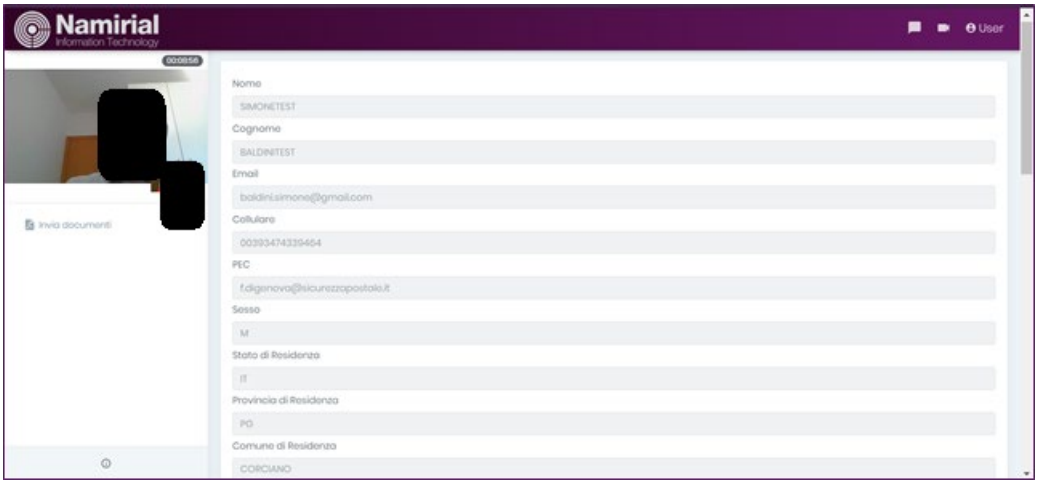


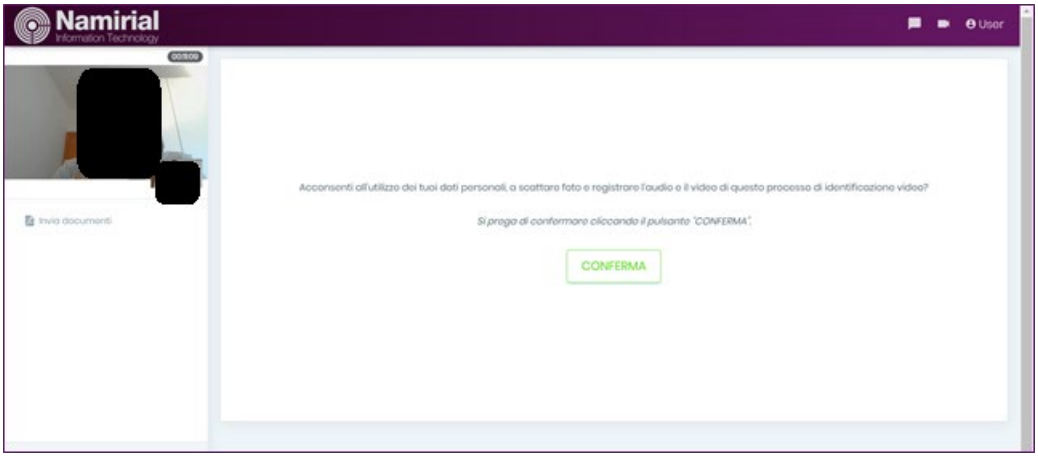
L'operatore raccoglie la chiamata e dà il benvenuto all'utente. Da questo momento viene avviato il processo di video riconoscimento.



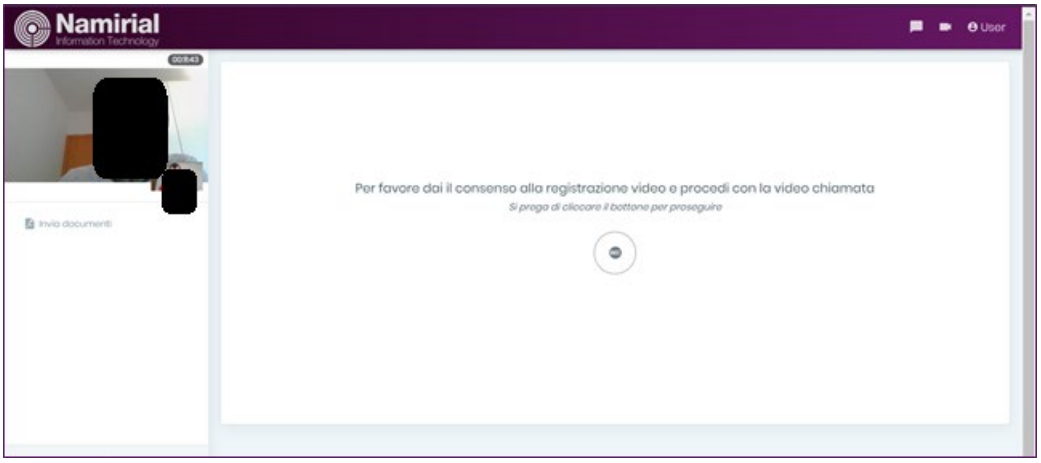
Step 3 - Conferma correttezza dati personali:

In questa fase l'operatore di riconoscimento chiede all'utente di confermare le proprie generalità invitandolo a verificare la correttezza dei dati riepilogati nella maschera. In caso contrario è possibile effettuarne la variazione.

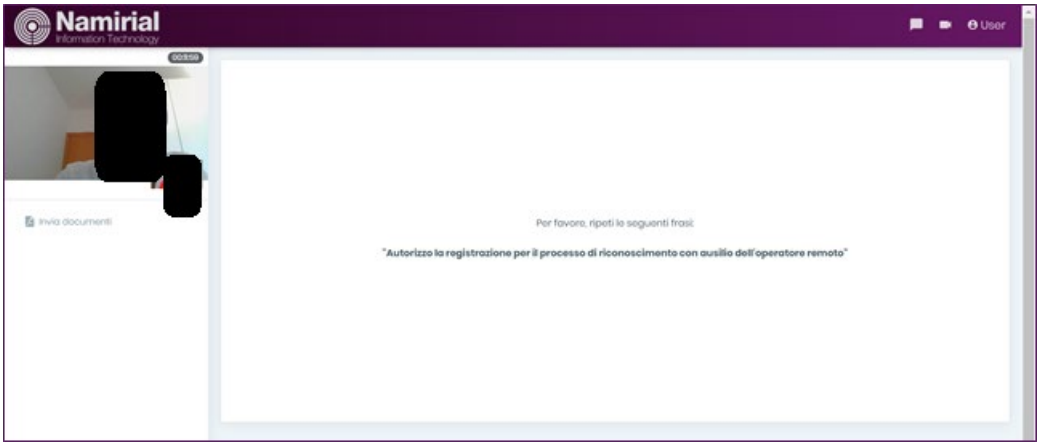




L'operatore di riconoscimento richiede il consenso al trattamento dei dati personali contenuti nelle riprese audio-video.



Step 4 – Acquisizione del consenso ed avvio della registrazione
Una volta raccolto il consento al trattamento dei dati, l'operatore informa che la videoregistrazione sarà conservata in modalità protetta e avvia la procedura.



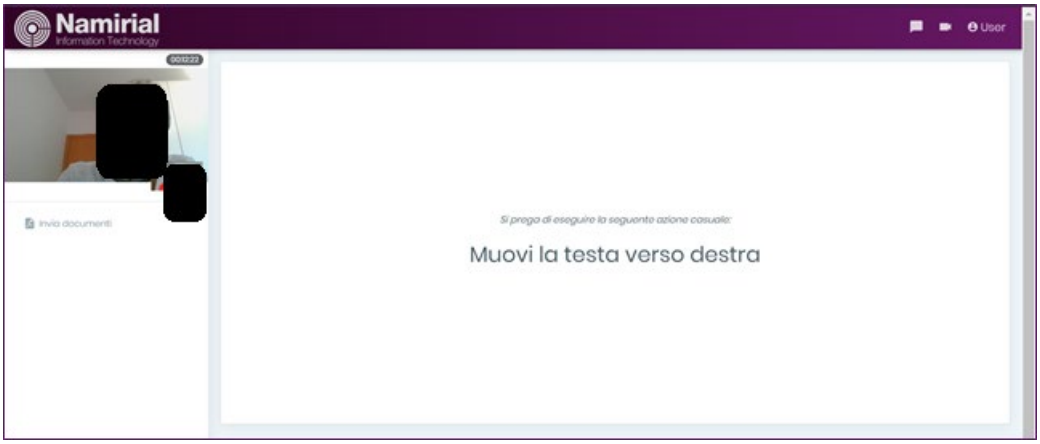
Step 5 - Presentazione dell'operatore
L'operatore inizia la procedura dichiarando i propri dati identificativi;

Step 6 - Conferme da parte dell'utente richiedente
L'operatore chiede esplicita conferma all'utente:

- della volontà di volersi dotare di un'identità digitale;
- della data ed ora della sessione di riconoscimento;
- dei dati inseriti nella modulistica online in fase di pre-registrazione;
- del proprio indirizzo email e del proprio numero di cellulare;
- Il luogo in cui si trova l'utente che sta richiedendo il riconoscimento;
- circa la conoscenza delle tipologie di credenziali di cui disporrà per l'accesso ai servizi in rete;

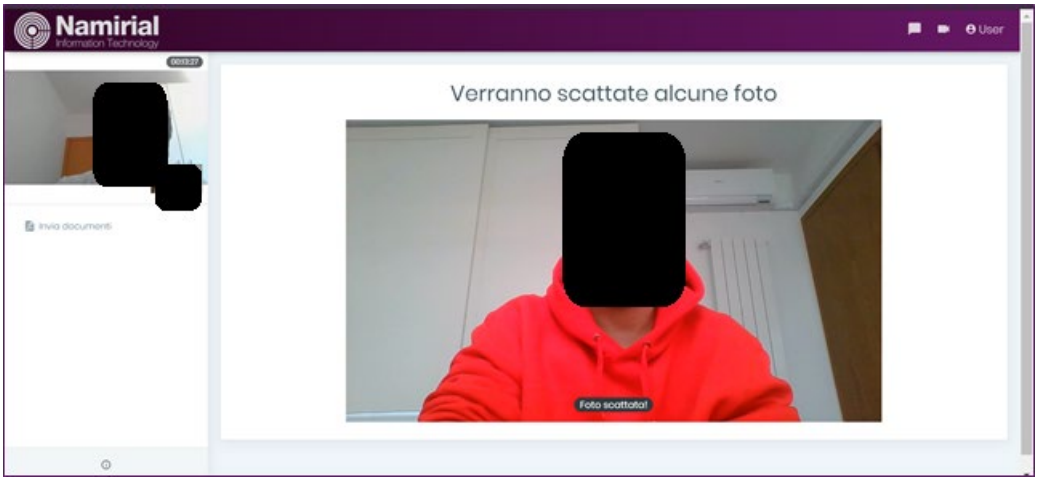
Se uno dei check sopraindicati non può essere completato, l'identificazione viene annullata dall'operatore.

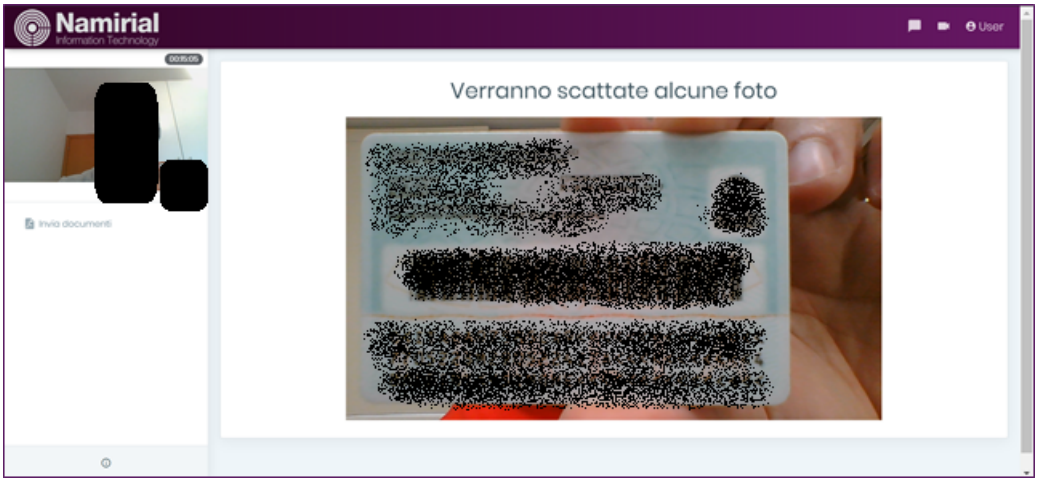
Step 7 – Azioni casuali
L'operatore chiede al soggetto di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta;

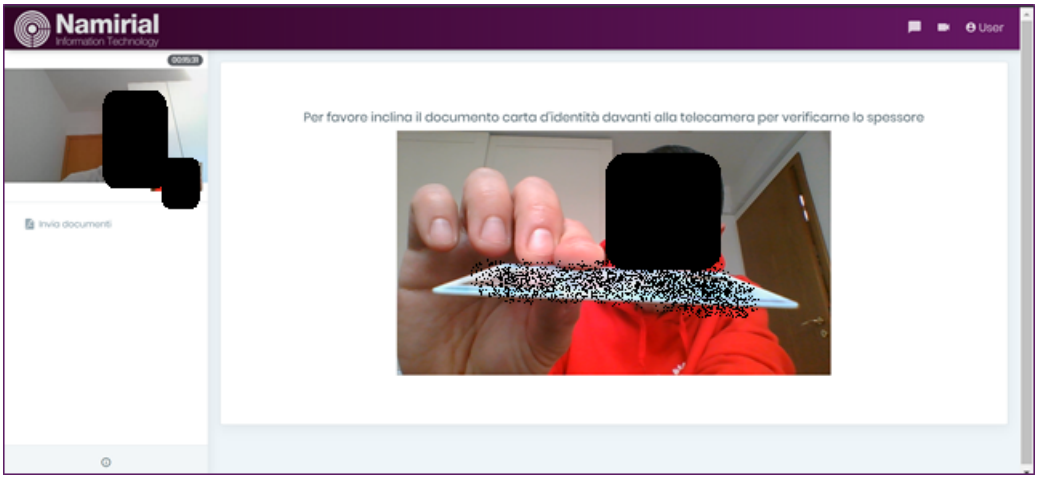


Step 8 – Geolocalizzazione
L'operatore effettua la geolocalizzazione del soggetto richiedente. Questa operazione è finalizzata al rafforzamento delle verifiche circa l'informazione sul luogo di svolgimento del riconoscimento dichiarato allo Step 6.

Step 9 – Verifica del documento di riconoscimento
L'operatore chiede di inquadrare il fronte ed il retro del documento di riconoscimento utilizzato dal soggetto, assicurandosi che sia possibile visualizzare chiaramente la fotografia e leggere tutte le informazioni contenute nello stesso (dati anagrafici, numero del documento, data di rilascio e di scadenza, amministrazione rilasciante);

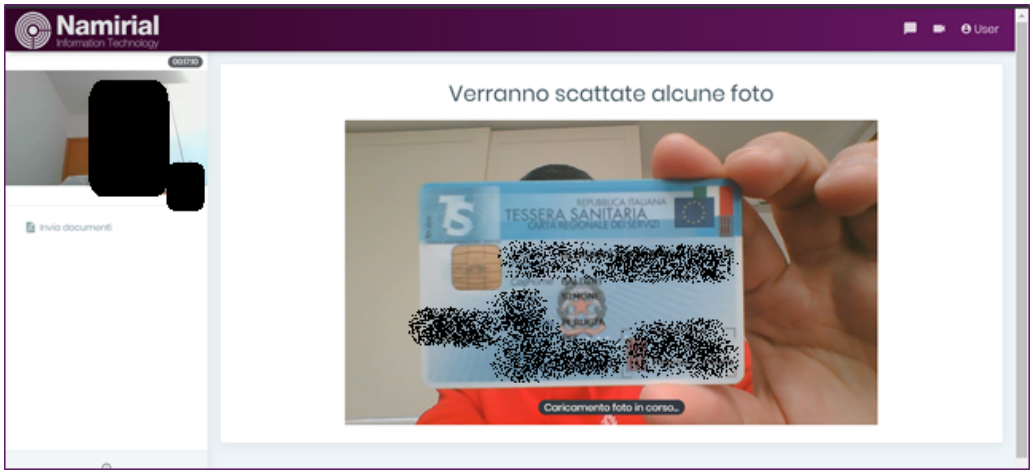


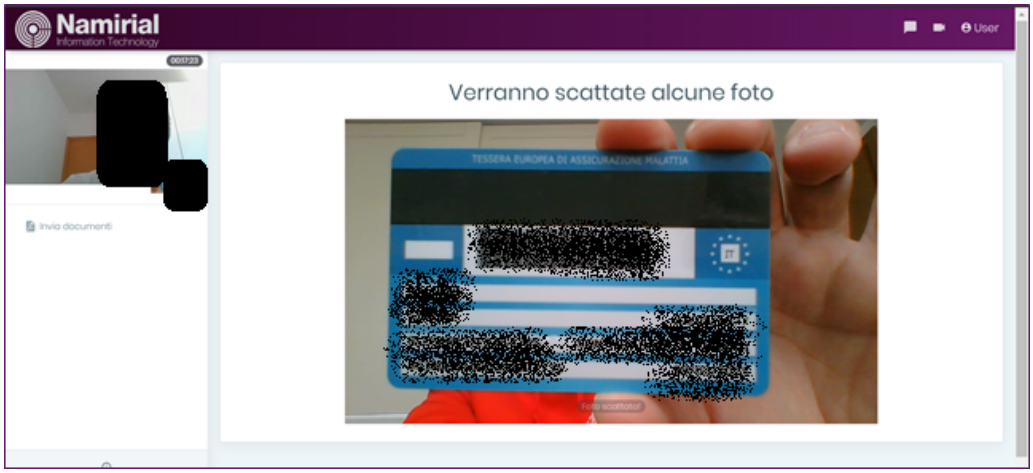


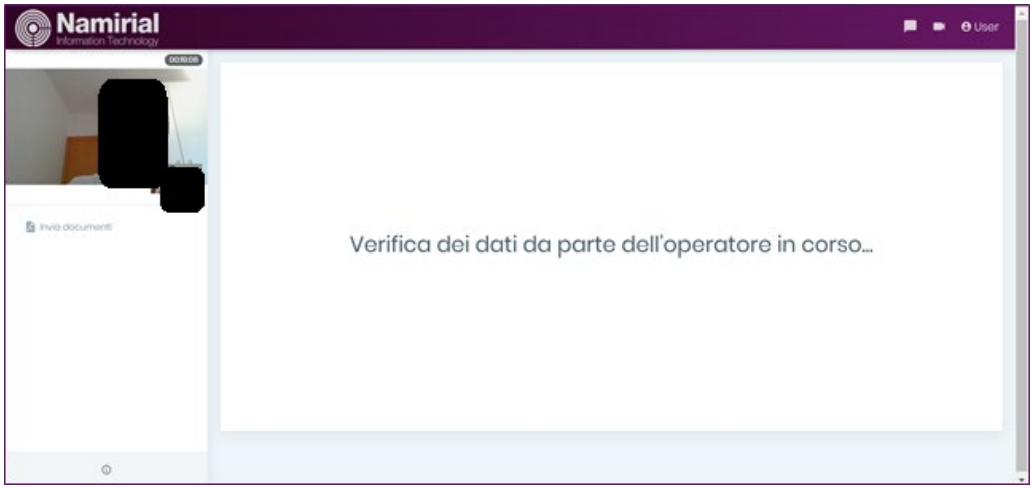


Step 10 – Verifica del Codice Fiscale

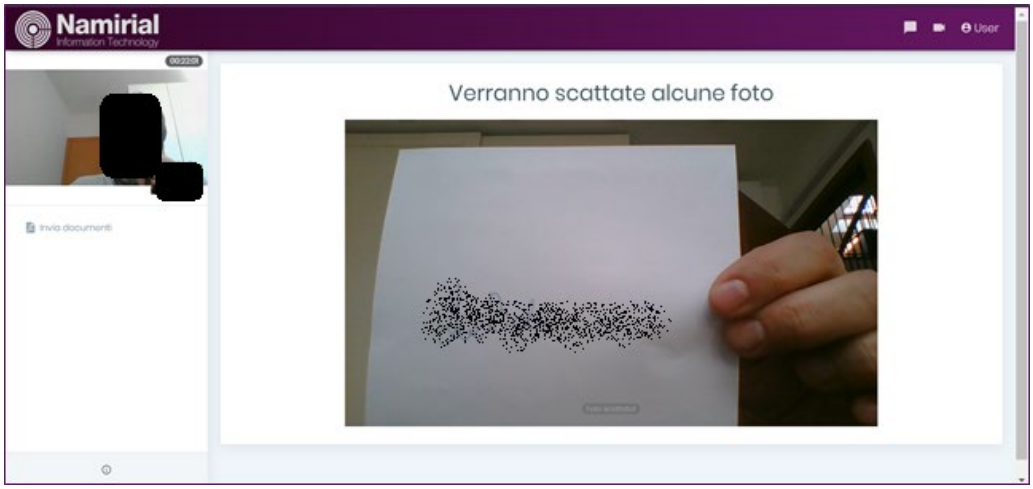
L'operatore chiede di mostrare la Tessera Sanitaria in corso di validità su cui è riportato il codice fiscale del soggetto.
In questa fase vengono acquisite delle foto della Tessera Sanitaria al fine di poter effettuare ulteriori verifiche da parte dell'operatore nel corso del video riconoscimento.

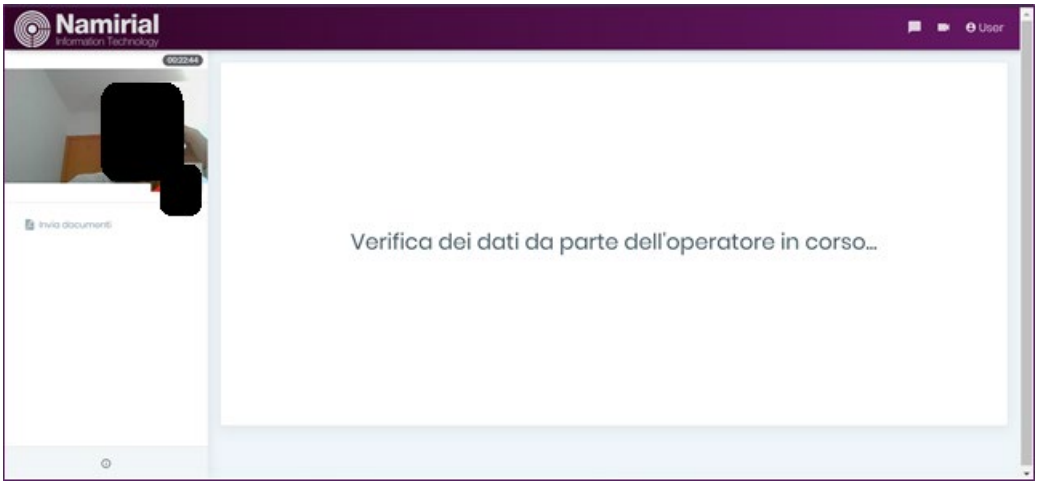




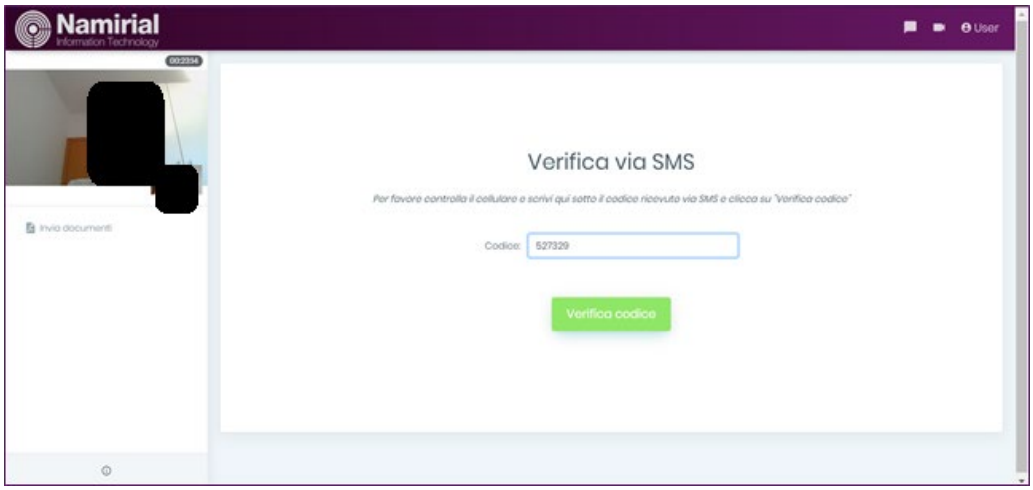


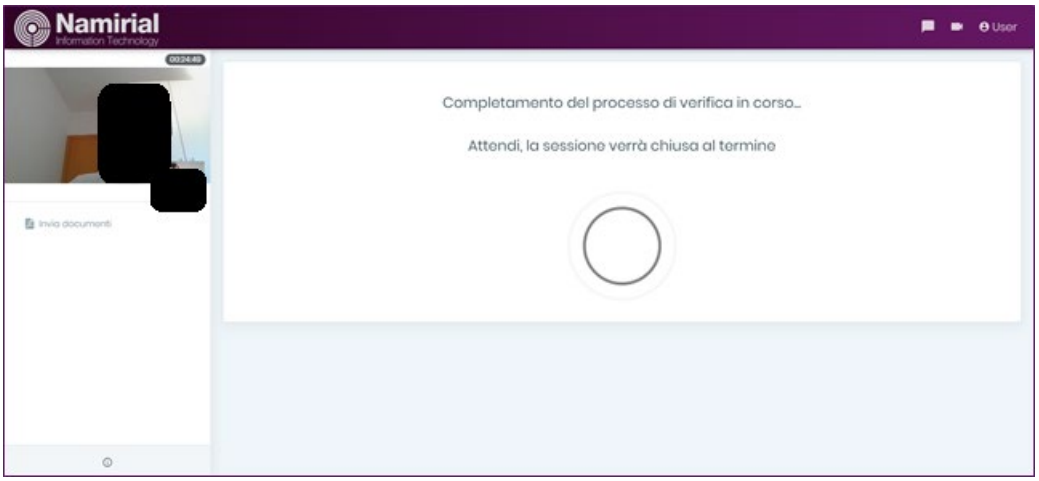
Step 11 – Acquisizione di una firma autografa e verifica
Quale ulteriore misura al rafforzamento della verifica dell'identità del richiedete, l'operatore chiede all'utente di applicare la propria firma su un foglio e mostrarla a schermo. La firma così acquisita verrà confrontata con quella contenuta nel documento di riconoscimento fotografato pochi istanti prima.





Step 12 – Verifica del cellulare e dell'email
L'operatore invia un sms che il soggetto richiedente è tenuto a verificare inserendolo nell'apposita maschera. L'operatore invia anche una mail all'indirizzo di posta elettronica dichiarato, con un link ad una URL appositamente predisposta per la verifica;

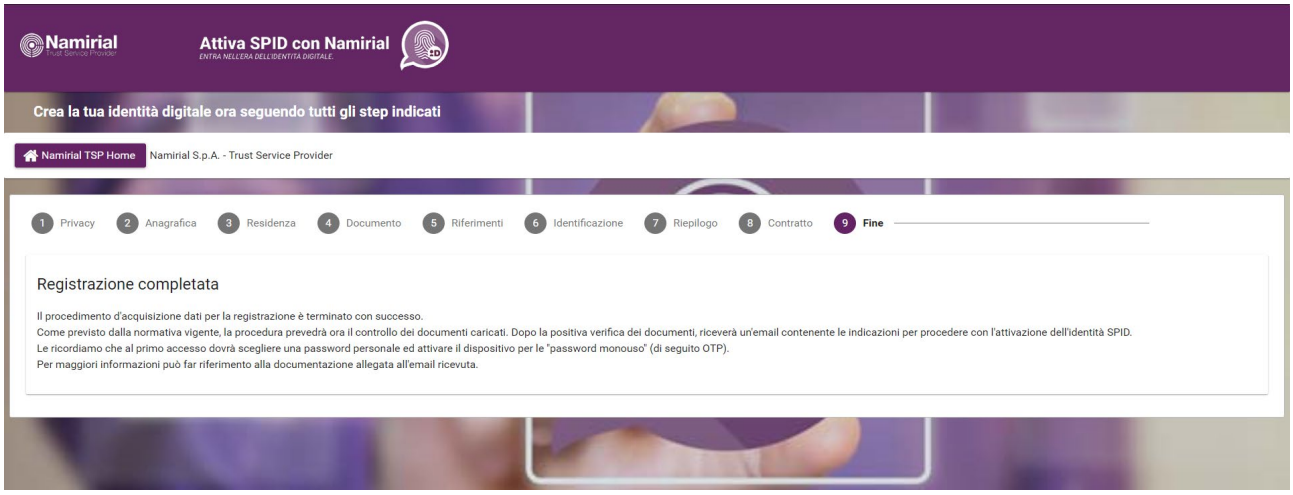


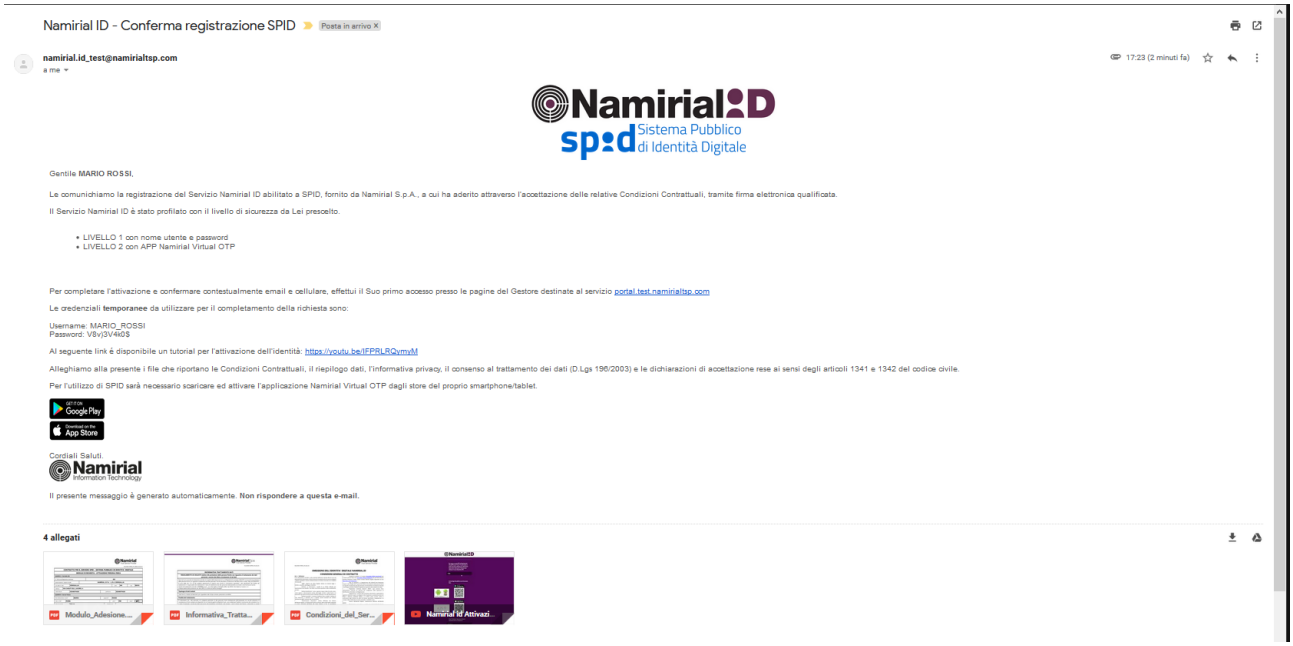


Step 12 – Conferme finali
Il soggetto conferma di aver preso visione e di accettare le condizioni contrattuali e d'uso disponibili sul sito web del gestore di identità. L'operatore riassume sinteticamente la volontà espressa dal soggetto di dotarsi di identità digitale e raccoglie conferma dallo stesso.

2.1.8 COMPLETAMENTO

In questa fase viene inviata un'e-mail alla casella registrata negli step precedenti. L'e-mail ha come oggetto "**Conferma Registrazione SPID**" e riporta un contenuto simile al seguente:





All'interno del messaggio è riportato il riepilogo delle principali informazioni sull'**Identità SPID e delle relative credenziali** e si fornisce un **codice segreto temporaneo** per completare l'attivazione dell'identità SPID.
All'interno del messaggio sono contenute anche le istruzioni per l'utente per completare l'attivazione dell'identità.
Il messaggio riporta in allegato il modulo di adesione, l'informativa sul trattamento dati e le condizioni generali di contratto.

2.1.9 ATTIVAZIONE

Seguendo le indicazioni contenute nell'email ricevuta l'utente accede ad una pagina in cui dovrà inserire username e password temporanea ricevuta per e-mail.

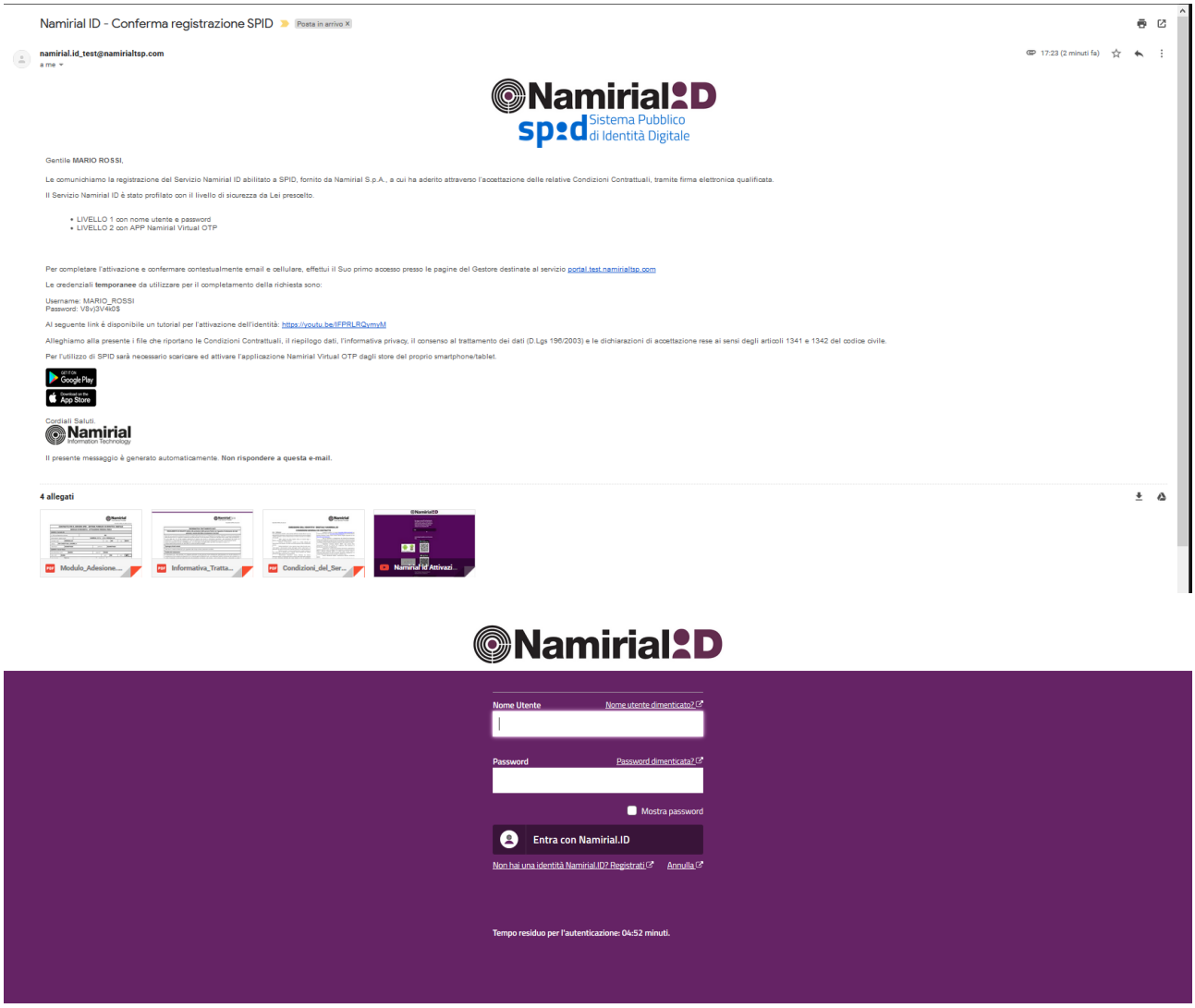


Figura 1 - Accesso SPID Namirial

All'interno di questa pagina viene chiesto l'inserimento del codice segreto temporaneo ricevuto per e-mail.
Se la verifica va a buon fine viene rilevato che l'utente è al suo primo accesso e viene invitato ad attivare le credenziali L2 e L1 con la procedura descritta nel seguito:

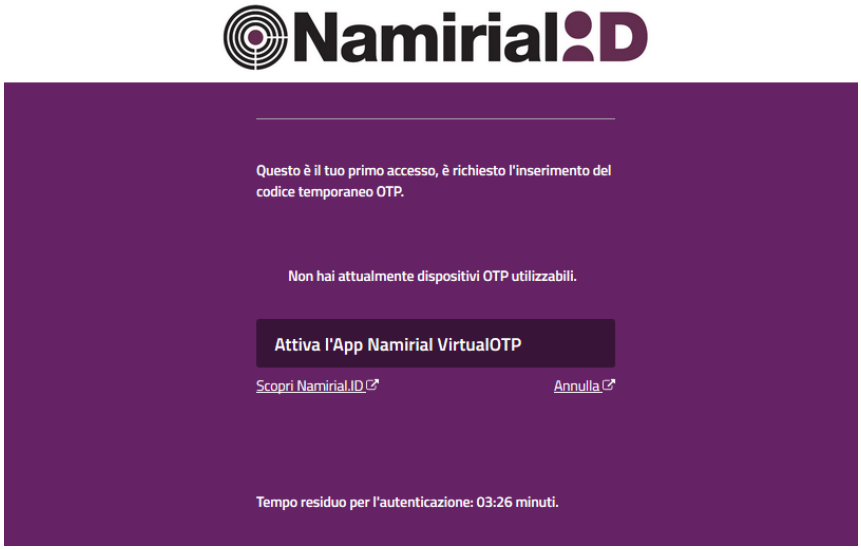
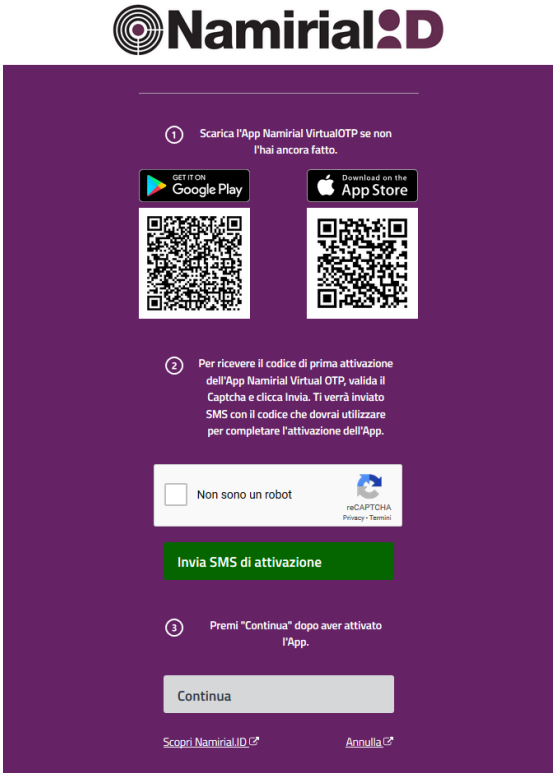
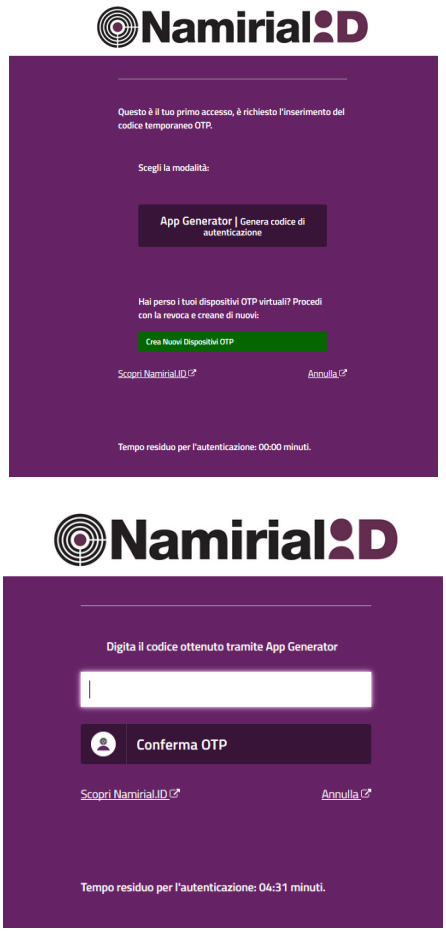


Figura 2 - Primo accesso SPID Namirial

L'utente è invitato ad installare e configurare l'applicazione Virtual OTP per gestire la credenziale di secondo livello



Cliccando su "non sono un robot" e chiedendo di ricevere l'sms di attivazione, l'utente deve proseguire cliccando sul bottone "continua". Nella schermata successiva è richiesto di inserire il codice OTP (si rimanda alla descrizione dell'attivazione della Virtual OTP):



Dopo che l'applicazione è stata correttamente configurata e dopo aver inserito il codice OTP generato dalla Virtual OTP, il sistema impone all'utente il cambio obbligatorio della password temporanea ricevuta in seguito all'attivazione dal parte del Gestore.

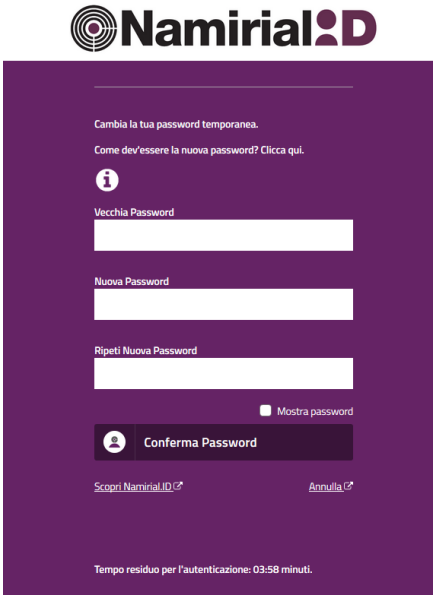


Figura 3 - Cambio Password SPID

Quando la procedura di attivazione termina con successo, il Gestore invia all'utente la mail che conferma l'avvenuta attivazione.

NB: è importante conservare questa e-mail in quanto contiene il Codice di Emergenza che l'utente deve utilizzare per le operazioni di revoca e/o cambio password.

- **Crea nuovo dispositivo OTP:** L'utente viene istruito sulla necessità di utilizzare il codice ricevuto per SMS per attivare l'App Namirial VirtualOTP seguendo il wizard mostrato dall'App stessa. L'App, una volta attivata, notificherà l'IdP consentendo all'utente di procedere con l'attivazione.

Completata la creazione dell'OTP viene mostrata una maschera in cui l'utente può scegliere con quale credenziale completare l'attivazione.

L'utente seleziona la credenziale desiderata e prosegue con l'autenticazione.

Nuova Password: inserire la password desiderata oppure ricorrere alla generazione casuale automatica tramite il link "Genera password random". In particolare, in relazione al tipo della password, la pagina raccomanda l'adozione di regole per ottenere password complesse e difficilmente attaccabili rispettando almeno i seguenti accorgimenti:

- lunghezza minima di otto caratteri;
- uso di caratteri maiuscoli e minuscoli;
- inclusione di uno o più caratteri numerici;
- non deve contenere più di due caratteri identici consecutivi;
- inclusione di almeno un carattere speciale (ad es #, $,% ecc).

Si raccomanda poi di vietare l'uso di informazioni non segrete riconducibili all'utente (ad es. codice fiscale, patente auto, sigle documenti, date, includere nomi, account-Id ecc.).
Conferma la password: inserire nuovamente la password inserita nel precedente campo (doppia conferma)

Nota: Si ricorda che la nuova password ha una durata di 180 giorni e non può essere riutilizzata

Se la password prescelta non è formalmente corretta verrà mostrato un messaggio di warning

Se la password risulterà formalmente valida, verrà confermato il cambio e si potrà completare il processo di attivazione dell'Identità e credenziali.

Cliccando sul tasto "Continua", verrà inviata un'email con oggetto **Attivazione identità SPID completata** all'indirizzo email precedentemente registrato
L'email contiene un riepilogo su:

- tipologia di credenziali attivate
- codice di emergenza per la gestione delle credenziali attivate
- allegati con condizioni contrattuali, copia del modulo sottoscritto e informativa privacy
- informazioni e riferimenti per ricevere assistenza

2.2 TIPOLOGIA DI CREDENZIALI FORNITE

2.2.1 LIVELLO 1

Per tale livello di autenticazione è richiesto di disporre dei soli parametri "**username**" e "**password**". In questo caso la procedura di attivazione (§ 2.1.12) abilita già l'utente al 1° livello di autenticazione SPID, pertanto non sono necessarie ulteriori operazioni di aggiunta delle credenziali.

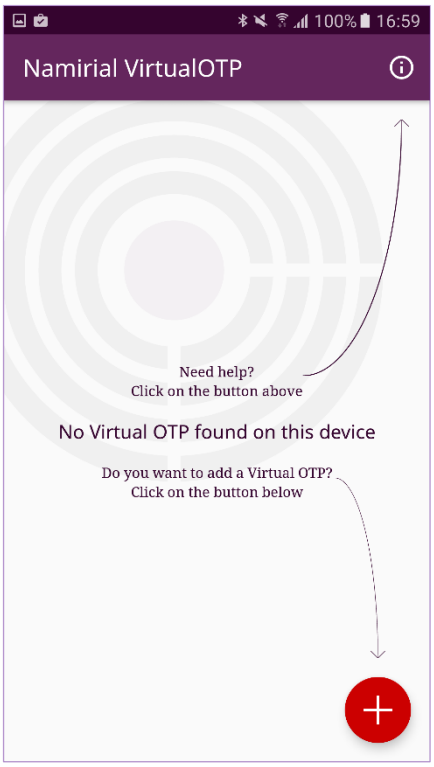
2.2.2 LIVELLO 2

Per tale livello di autenticazione è richiesto l'utilizzo di un **codice OTP** (**One Time Password**) – oltre che di una "**username**" e "**password**".

E' possibile selezionare la tipologia di credenziale OTP che si intende utilizzare tra quelle disponibili a video, tra cui:

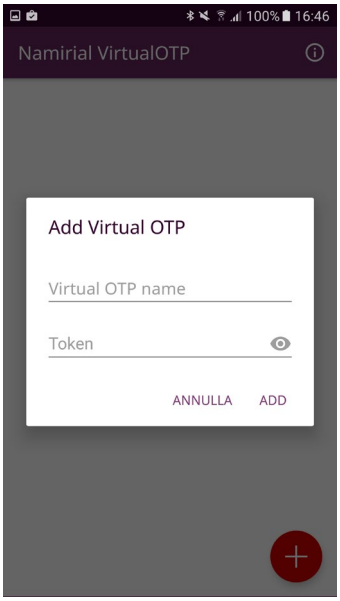
- OTP mobile
- OTP SMS

OTP App
Per utilizzare l'autenticazione di secondo livello, l'utente può utilizzare l'App OTP per Android o iOS, gratuitamente scaricabile dagli Store Google Play e App Store.



Per attivare l'App è necessario che l'utente abbia a disposizione l'email ricevuta a seguito dell'identificazione e il cellullare registrato in fase di richiesta.

1. la prima schermata invita l'utente ad effettuare il primo accesso alle pagine di attivazione del servizio SPID. Le informazioni sono contenute nell'email ricevuta a conclusione del processo di attivazione (§ 2.1.11)
2. L'utente accede ad una maschera di verifica inserisce il codice ricevuto per email e procede
3. Se l'autenticazione va a buon fine viene inviato al numero di telefono cellulare un codice di verifica. *"TSP Namirial S.p.A. – SPID Codice di attivazione App iOS/Android: <codice>*
4. Con il codice ricevuto è possibile confermare la credenziale inserendo il valore nel campo dell'App e confermare premendo il tasto "Add".



5. Se l'inserimento è corretto, l'App si attiva e richiede la scelta di un codice di sblocco da utilizzare per confermare la richiesta dell'OTP. In alternativa al codice, per gli smartphone che lo prevedono, è possibile anche utilizzare il meccanismo del fingerprint che consente lo sblocco del telefono con l'impronta digitale oppure il meccanismo nativo di sblocco del device eventualmente impostato dall'utente: gesture, pin, password.

OTP SMS

In alternativa all'uso dell'App Namirial prevede l'adozione di codici OTP con SMS inviati sul numero registrato in fase di identificazione.
In questo caso la parte di dispositivo personale è rappresentata dal cellulare in cui il Gestore invia i codici one-time.
La registrazione di questo tipo di credenziale prevede l'inserimento del codice di attivazione ricevuto per SMS al numero di telefono precedentemente registrato e verificato.
Con il codice ricevuto è possibile confermare la credenziale inserendo il valore nel campo richiesto e confermare premendo il tasto Conferma OTP
A questo punto l'operazione aggiunta della credenziale può ritenersi conclusa con successo.

3 UTILIZZO DELL'IDENTITÀ SPID

L'utente, collegato al Service Provider desiderato, si trova a dover accedere a uno dei suoi servizi con la propria Identità SPID. Si rammenta che l'Identità SPID permette l'accesso ad aree private e sicure o a servizi di terze parti, che siano Pubblica Amministrazione o soggetti privati. Indipendentemente da quale sia il fornitore di servizi, la form di connessione mostra sempre:

- La lista degli IdP accreditati, da cui scegliere il proprio (**Namirial.ID** nella fattispecie)
- Il livello SPID minimo necessario per poter accedere al servizio

Di seguito una immagine usata come esempio:

Figura 4 - Accesso Servizi PA con SPID

La selezione del livello di autenticazione avviene cliccando sopra l'icona corrispondente, che innesca la procedura di login coerente con il livello indicato:

- Accesso SPID con autenticazione di livello 1
- Accesso SPID con autenticazione di livello 2

3.1 ACCESSO CON LIVELLO 1

Figura 5 - Accesso SPID L1 Namirial

L'autenticazione per l'accesso SPID con livello 1 richiede che l'utente sia provvisto dei seguenti parametri di accesso:

- Username
- Password

I parametri necessari sono quelli che soddisfano le credenziali di accesso di livello 1.
Una volta inseriti i dati della credenziale, confermare premendo il taso "Entra con SPID".
Verrà generato, in maniera del tutto trasparente, un flusso di informazioni tra il Service Provider e l'IdP che porterà ai seguenti risultati:

Nel caso di esito positivo:

- L'accesso al servizio richiesto, previa accettazione dell'informativa sulla trasmissione dei dati al service provider
- La ricezione, da parte del cliente, della comunicazione via email contenente gli estremi relativi all'autenticazione effettuata:

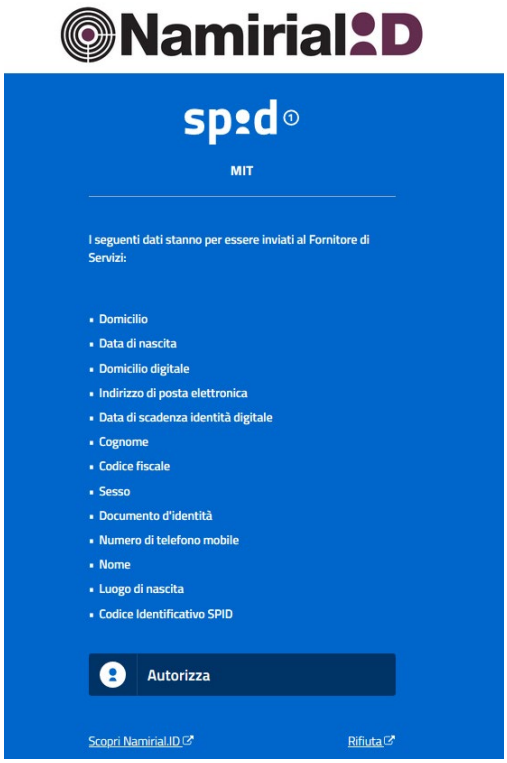


Figura 6 - Accesso SPID L1: Notifica attributi richiesti dal SP

In caso di esito negativo viene restituito un codice di errore all'utente e, ovviamente, impedito l'accesso al servizio richiesto.

3.2 ACCESSO CON LIVELLO 2

L'autenticazione per l'accesso SPID con livello 2 richiede – in analogia al livello 1 - che l'utente sia provvisto dei seguenti parametri di accesso:

- Username
- Password

In aggiunta è necessario che l'utente abbia associata almeno una delle seguenti tipologie di credenziali:

- OTP mobile
- OTP SMS

La prima fase di accesso ad un servizio di livello 2 vede l'utente invitato ad inserire i parametri SPID di Username e Password

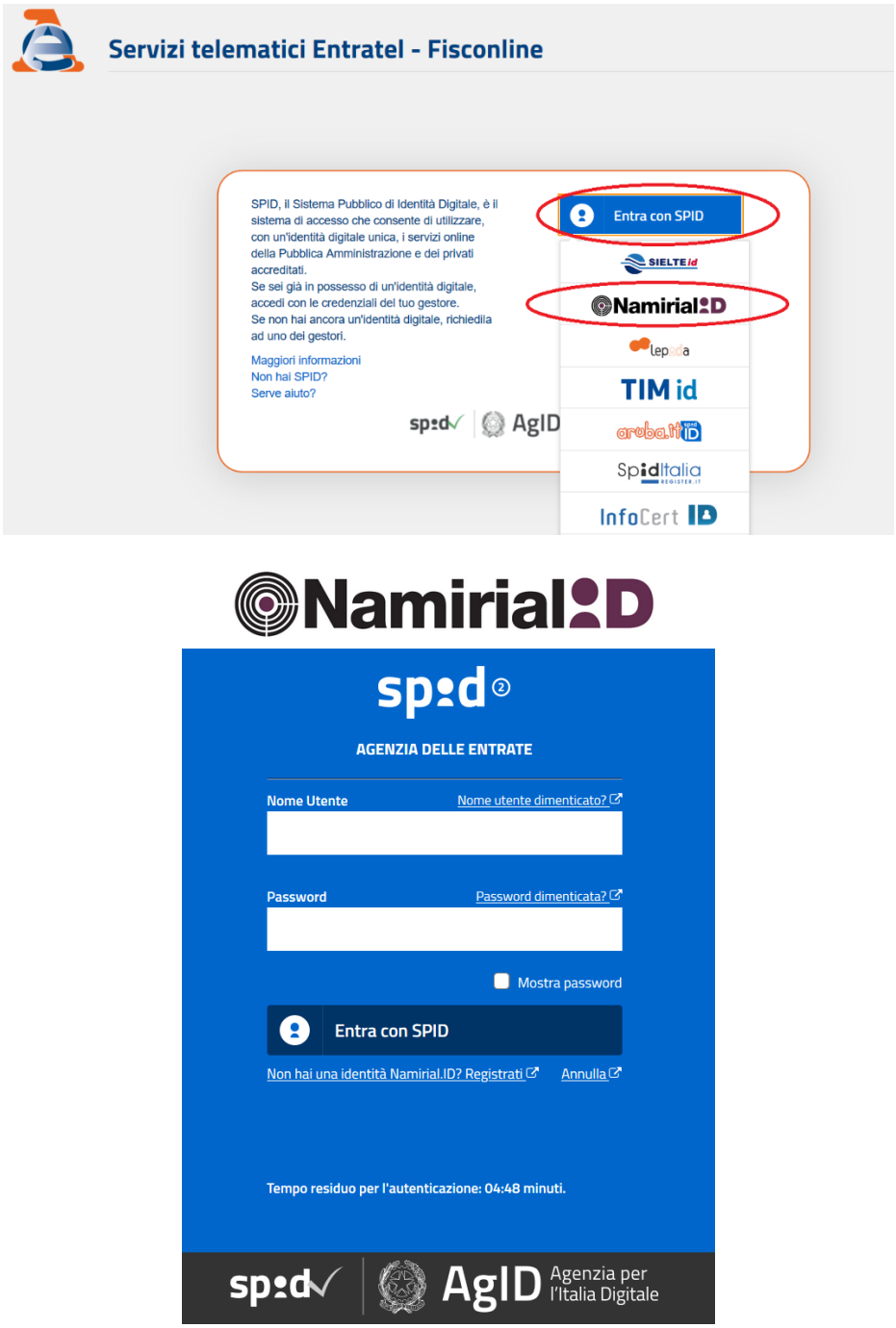


Figura 7 - Accesso L2 SPID Namirial: user e password

Si confermeranno i valori premendo il pulsante “Entra con SPID”.

Se la prima fase di autorizzazione ha esito positivo verrà mostrata una pagina dalla quale poter scegliere la credenziale di livello 2 necessaria per l’accesso ai servizi desiderati.

Figura 8 - Accesso L2 SPID Namirial: selezione dell'OTP

Si noti che le credenziali visibili sono solo quelle realmente associate all'Identità e non tutte quelle offerte dal Gestore IdP. Una volta selezionata la credenziale desiderata verrà richiesto il codice OTP (One Time Password) necessario all'autenticazione vera e propria:

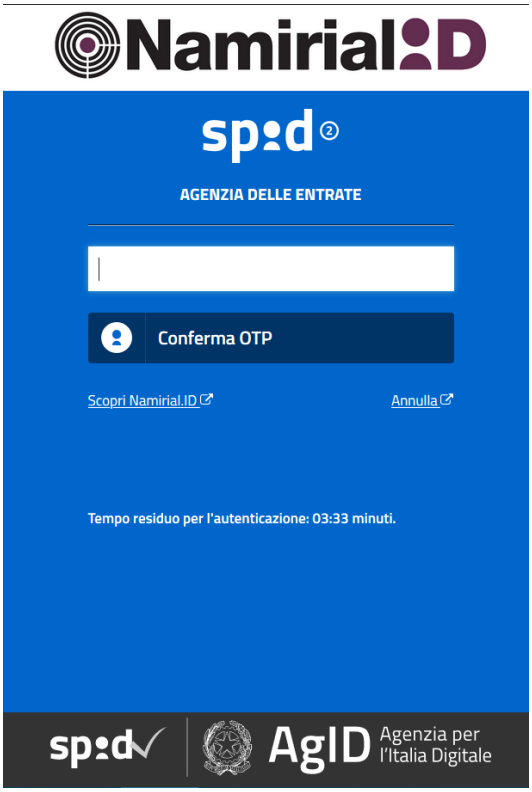


Figura 9 - Accesso L2 SPID Namirial: inserimento OTP

La tipologia di credenziale differisce fondamentalmente per il canale di trasmissione dei codici di autenticazione all'utente richiedente:

- applicazione mobile per OTP
- messaggio SMS

Il completamento della procedura di autenticazione si ottiene con il corretto inserimento dell'OTP e premendo il tasto per la Conferma.
Viene generato, in maniera del tutto trasparente, un flusso di informazioni tra il Service Provider e l'IdP che restituisce i seguenti risultati:

Nel caso di esito positivo:

- L'accesso al servizio richiesto, previa accettazione dell'informativa sulla trasmissione dei dati al service provider
- La ricezione, da parte del cliente, della comunicazione via email contenente gli estremi relativi all'autenticazione effettuata.

Figura 10 - Accesso SPID L2: Notifica attributi richiesti dal SP

In caso di esito negativo viene restituito un errore all'utente e, ovviamente, impedito l'accesso al servizio richiesto.

.

4 GESTIONE DELL'IDENTITÀ SPID

4.1 ACCESSO ALL'AREA UTENTE

Il Gestore mette a disposizione un'Area Utente all'interno del proprio portale in cui gli utenti, previa autenticazione di livello 2 posso operare autonomamente ai fini della gestione delle proprie identità/credenziali.

Il portale è raggiungibile al link al seguente link: https://portal.namirialtsp.com/
https://portal.namirialtsp.com/

Figura 11 - Area gestione SPID

All'interno dell'Area sono rese disponibili le funzioni descritte ai paragrafi successivi.
Per accede alla propria area utente, è necessario fare click su "ACCEDI" e compilare i campi che vengono proposti (vedi schermata successiva):

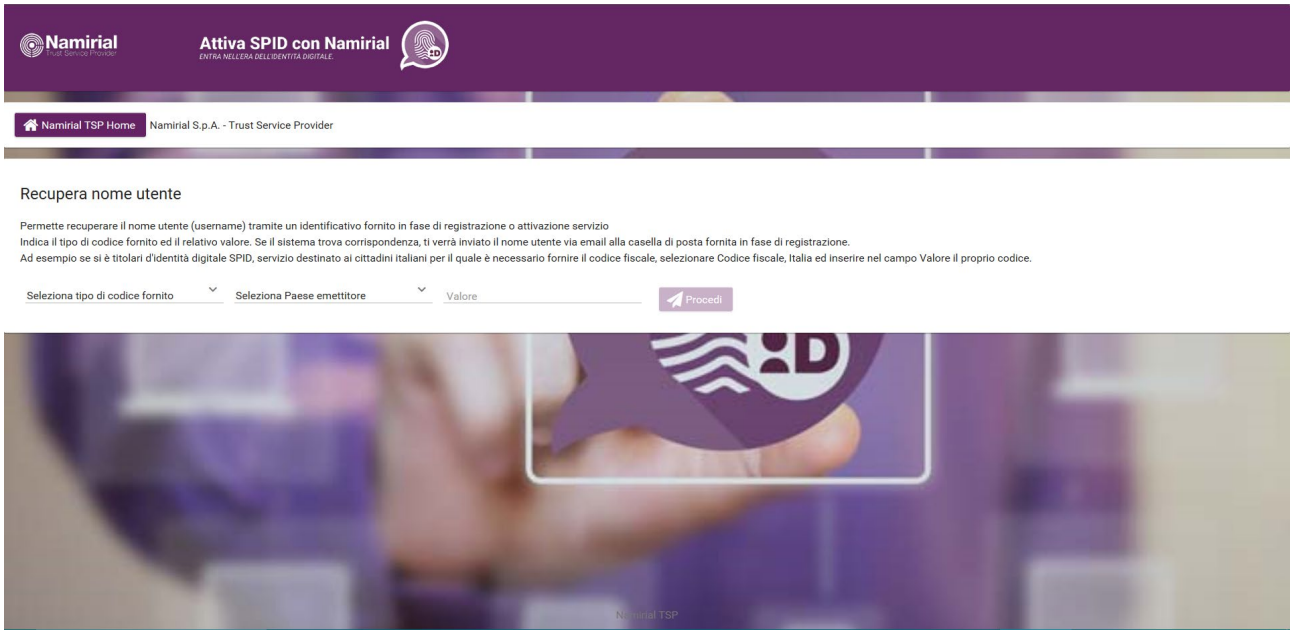
E' previsto un tempo di sessione di 5 minuti per eseguire la login.
Se la login va a buon fine, l'utente accede alla propria area privata che si presenta come segue:

Qualora l'utente non ricordi le credenziali (Username e/o Password) sono disponibili due funzioni:

- "Non ricordo il nome utente", per il recupero dello username
- "Non ricordo la password", per il recupero della crendenziale di livello 1 (L1)

4.1.1 "NON RICORDO IL NOME UTENTE"

La funzione permette di recuperare il nome utente (username) tramite un identificativo fornito in fase di registrazione o attivazione servizio. L'utente deve indicare il tipo di codice fornito ed il relativo valore. Se il sistema trova corrispondenza, verrà inviato il nome utente via email alla casella di posta fornita in fase di registrazione.



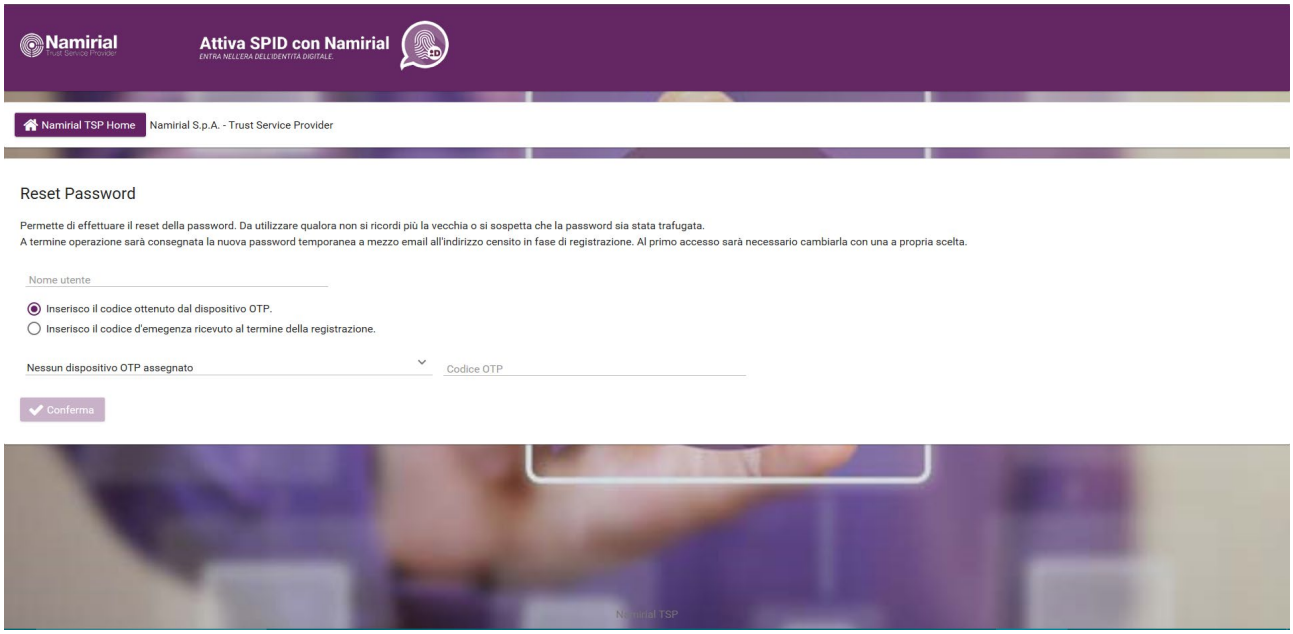
I valori possibili per il tipo di codice fornito sono:

- Codice Fiscale
- Numero della Carta di Identità
- Passaporto

In base al codice selezionato, la funzione chiede di indicare il Paese emettitore e successivamente il valore del codice.
Se la procedura va a buon fine, l'utente riceverà una mail con oggetto "Namirial ID - Richiesta recupero username" e nel corpo della mail viene indicata la username.

4.1.2 "NON RICORDO LA PASSWORD"

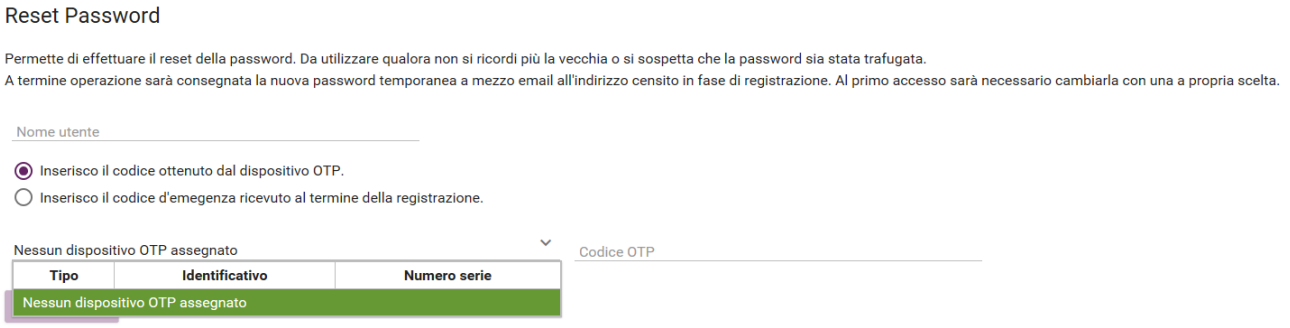
La funzione permette di effettuare il reset della password ed è da utilizzare qualora non si ricordi più la vecchia o si sospetta che la password sia compromessa. Al termine dell'operazione l'utente riceve una nuova password temporanea a mezzo e-mail all'indirizzo censito in fase di registrazione. Al primo accesso, il sistema richiede un cambio obbligatorio con una a propria scelta.



Per resettare la password è obbligatorio indicare il nome utente (cfr paragrafo precedente) e uno tra i due dei seguenti valori:

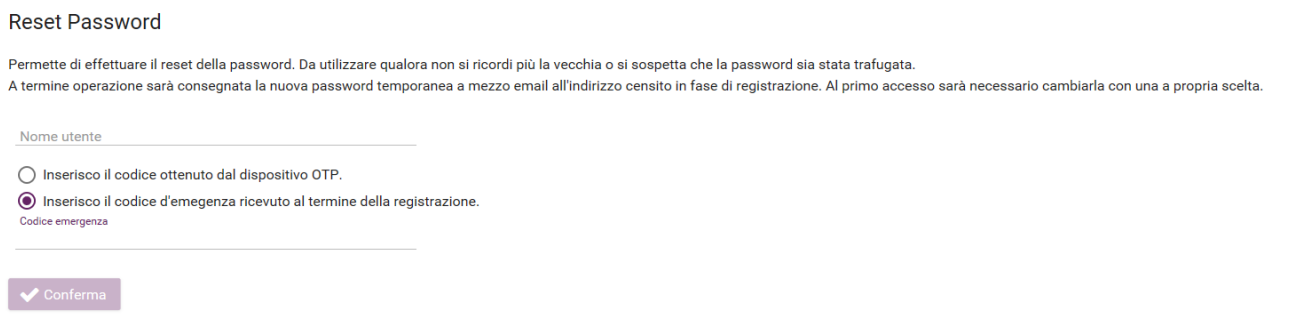
- Codice OTP (è necessario aver configurato l'apposita applicazione Virtual OTP)
- Codice di Emergenza (ricevuto al termine della registrazione mediante e-mail).

Se l'utente decide di utilizzare il Codice OTP, viene fornita la lista dei dispositivi associati alla username indicata (come mostra la seguente immagine generica):



Nota: i valori riepilogati nella colonna "Identificativo" sono riscontrabili nella lista dei dispositivi virtuali dell'applicazione (cfr sezione relativa all'uso dell'app Virtual OTP)

Se l'utente decide di usare il codice di emergenza ricevuto via e-mail, allora la schermata si presenta come segue:



Quando l'utente ha a disposizione le proprie credenziali e si autentica correttamente, il sistema restituisce la seguente schermata (che rappresenta la "Home" dell'utente):

4.2 SOSPENSIONE E REVOCA DELL'IDENTITÀ DIGITALE

L'utente che intende **Revocare** o **Sospendere** la propria identità SPID potrà effettuare la procedura all'interno dell'area web dedicata resa disponibile dal Gestore Namirial. Le funzioni di Revoca e Sospensione dell'Identità sono attivabili solo previa autenticazione di livello massimo tra quelle fornite dal Gestore.

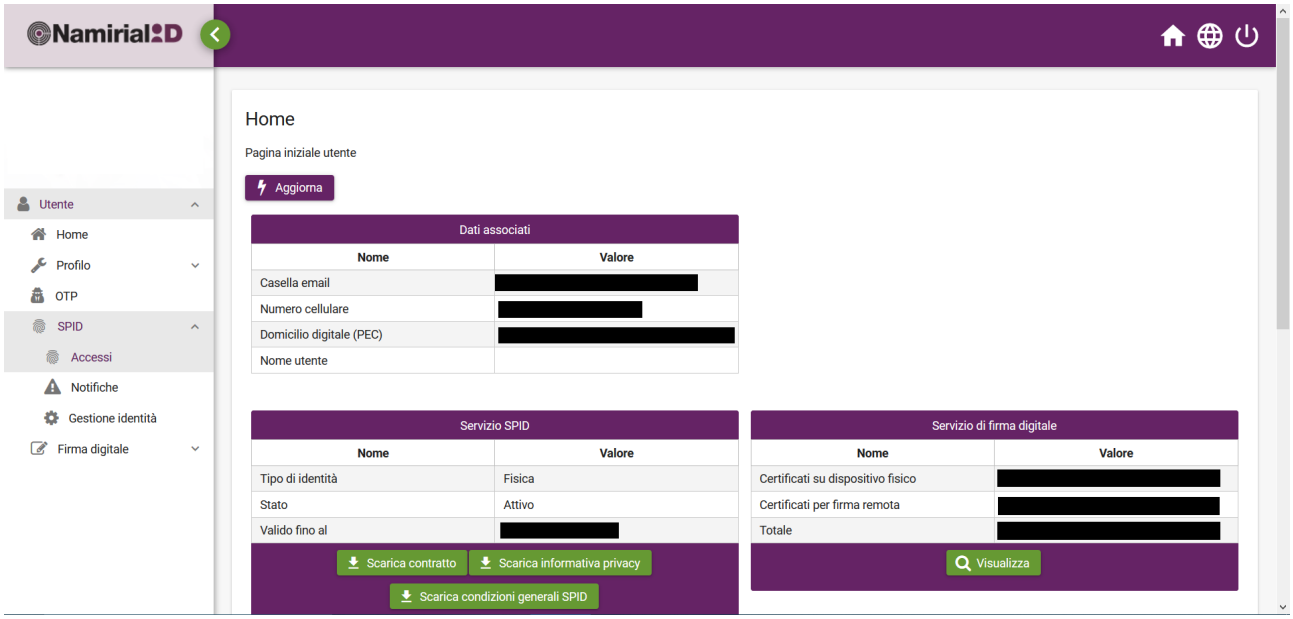
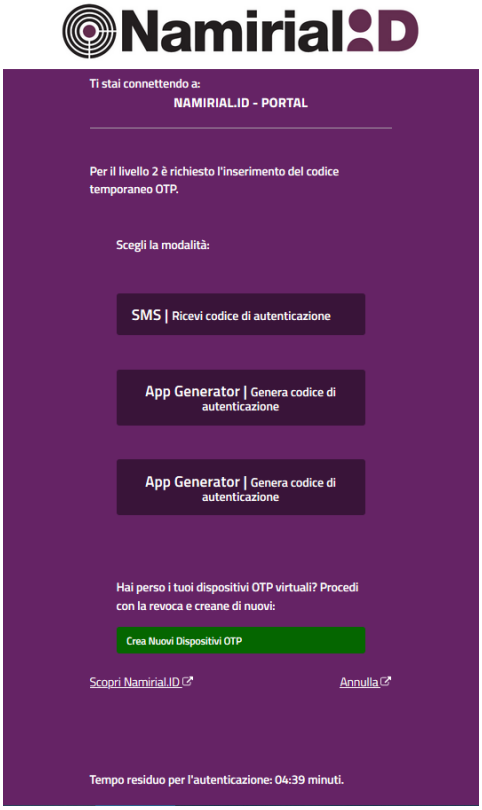


Figura 12 - SPID Namirial: Home page dell'utente sul portale di gestione

L'utente che intende dunque procedere con la **Sospensione** dell'Identità attiva l'apposita funzione utilizza la voce di menù "Gestione Identità" del gruppo SPID e viene indirizzato sulla pagina di autenticazione del Gestore che forza l'autenticazione di livello 2.Inserendo le credenziali apposite, il sistema propone la seguente schermata:



NB: in base al numero di dispositivi che l'utente ha richiesto, questi gli vengono elencati. La scelta di uno tra questi non pregiudica le operazioni di autenticazione a patto di inserire correttamente il codice OTP.

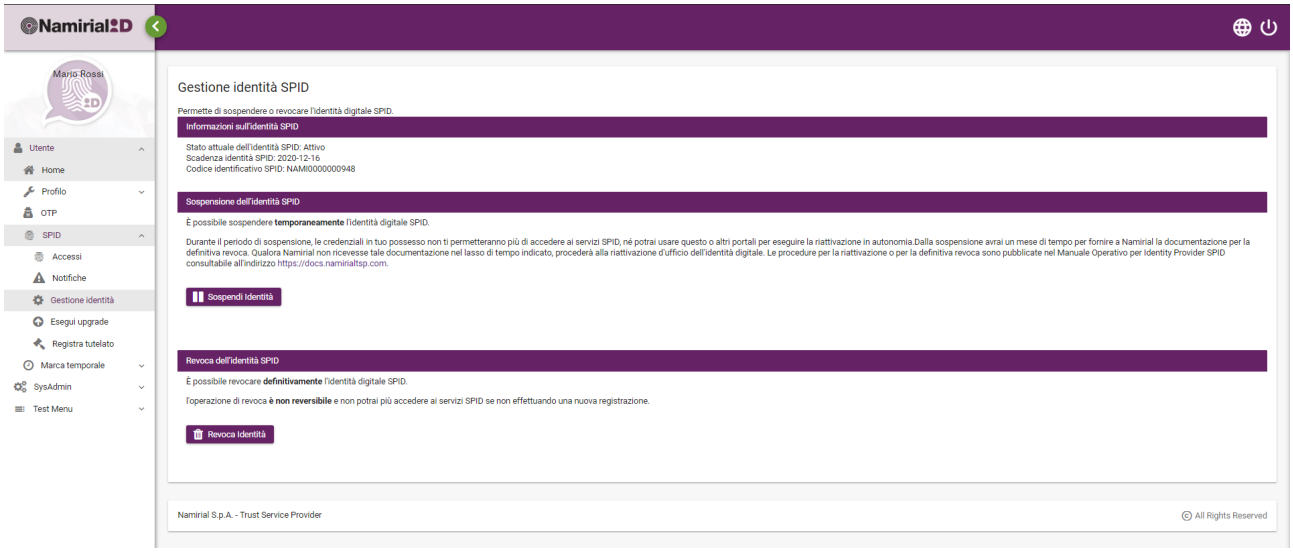
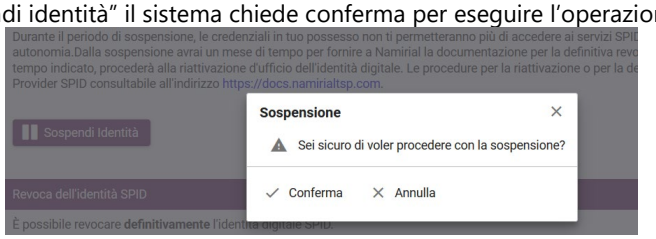
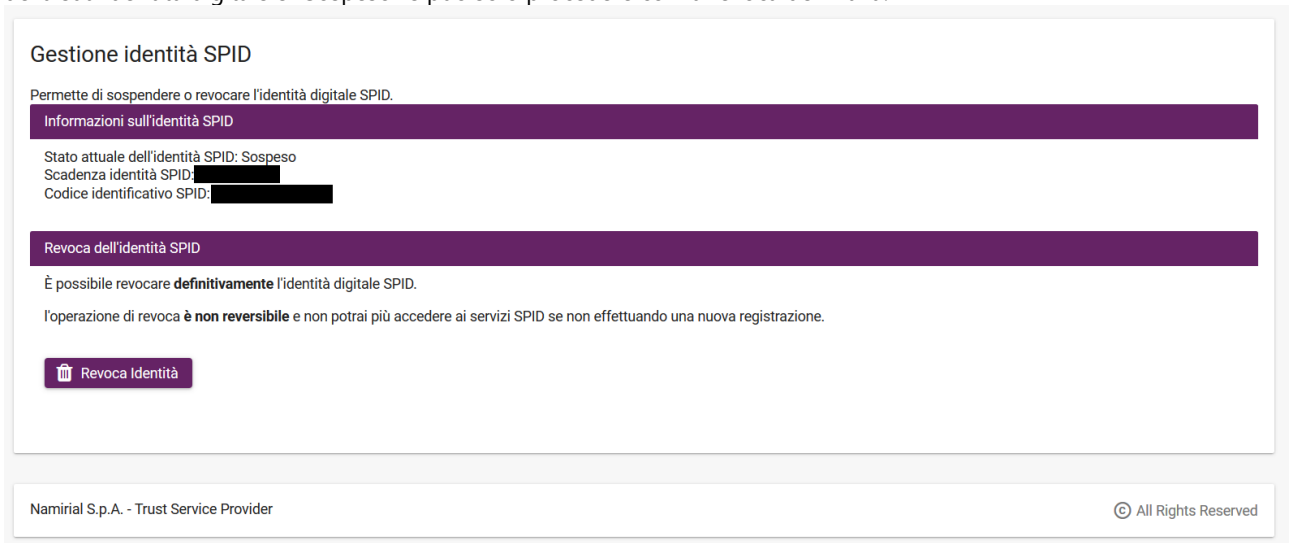


Figura 13 - SPID Namirial: Sospensione con Livello 2

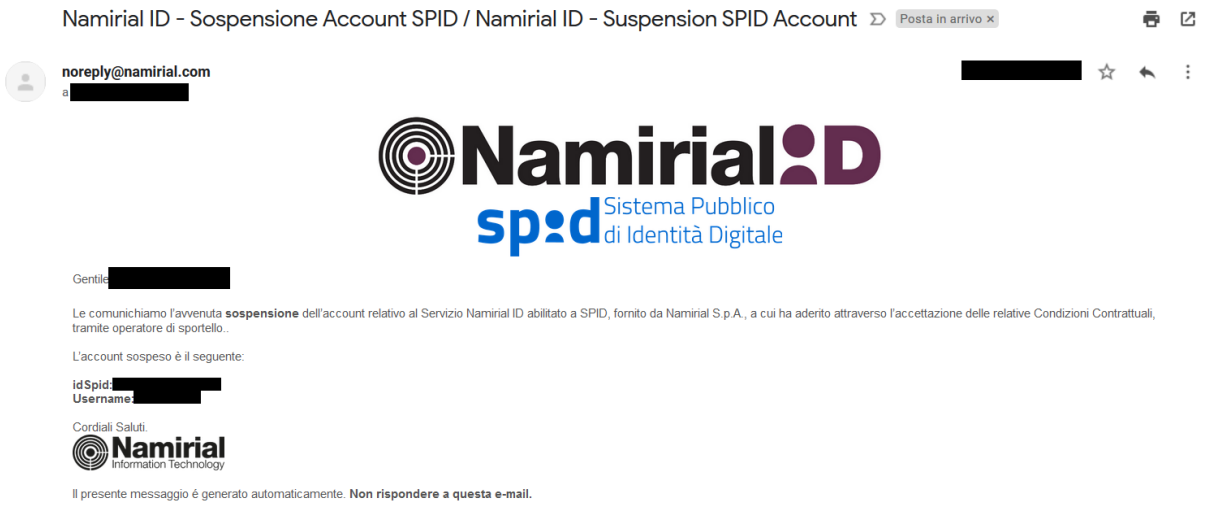
Cliccando sul bottone "Sospendi identità" il sistema chiede conferma per eseguire l'operazione:



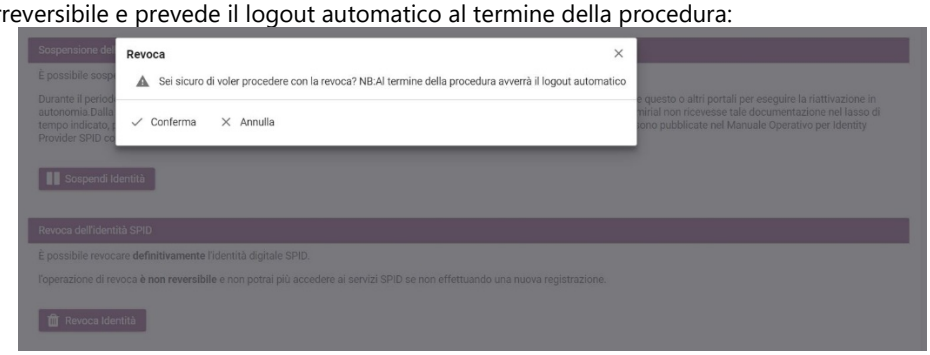
Al termine della procedura, l'utente viene indirizzato sulla pagina di Gestione dell'identità dove viene avvisato che lo stato della sua identità digitale è "Sospeso" e può solo procedere con la revoca definitiva.



Contestualmente alla sospensione, il Gestore avvisa l'utente dell'avvenuta operazione inviando all'indirizzo mail verificato in fase di registrazione la seguente mail:



La funzione di **Revoca** dell'Identità segue la stessa procedura e gli stessi criteri di autenticazione utilizzati per la sospensione, ma presenta un messaggio di conferma diverso dalla sospensione in quanto la revoca dell'identità è un'operazione irreversibile e prevede il logout automatico al termine della procedura:



Come per la sospensione, il sistema invia in automatico un messaggio all'indirizzo di posta elettronica verificato in fase di registrazione comprovante l'esito dell'azione di revoca.

Oltre ai meccanismi disponibili dal Portale, così come previsto dal Regolamento [VIII], sono rese disponibili le seguenti modalità di inoltro della richieste di Revoca e/o Sospensione:

a) richiesta al gestore inviata via PEC[1] alla seguente casella namirial.id@sicurezzapostale.it;
b) richiesta inviata alla casella namirial.id@namirialtsp.com tramite la casella di posta nota al gestore in formato elettronico e sottoscritta con firma digitale
c) richiesta inviata alla casella namirial.id@namirialtsp.com, tramite casella di posta elettronica diversa da quella nota al gestore, allegando la scansione del modulo di richiesta di revoca o sospensione firmato e copia del documento d'identità

A titolo informativo si ricorda che, ai sensi dell'articolo 8, comma 3 e dell'articolo 9 del [II], il gestore revoca l'identità digitale nei casi seguenti:

1. risulta non attiva per un periodo superiore a 24 mesi;
2. per decesso della persona fisica;
3. per estinzione della persona giuridica;
4. per uso illecito dell'identità digitale;
5. per richiesta dell' utente;
6. per scadenza contrattuale;
7. per scadenza documento identità;

Nei casi previsti dai punti 1 e 6, il gestore dell'identità digitale revoca di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica la causa e la data della revoca all'utente, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica registrato come attributo secondario.
Nei casi previsti dai punti 2 e 3, il gestore dell'identità digitale procede alla revoca dell'identità digitale, previo accertamento operato anche utilizzando i servizi messi a disposizione dalle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM.
In assenza di disponibilità dei predetti servizi, dovrà essere cura dei rappresentanti del soggetto utente (eredi o procuratore, amministrazione, società subentrante) presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'identità digitale. Il gestore, una volta in possesso della documentazione suddetta, dovrà procedere tempestivamente alla revoca.
Nel caso previsto dal punto 7, il gestore dell'identità digitale sospende di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica la causa e la data della sospensione all'utente, utilizzando l'indirizzo di posta elettronica registrato come attributo secondario.

A seguito della richiesta di sospensione dell'identità SPID Namirial fornirà esplicita evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla sospensione dell'identità digitale. Contestualmente l'utente potrà richiedere al fornitore dei servizi presso il quale ritiene che la propria identità sia stata utilizzata fraudolentemente il blocco all'accesso della propria identità inviando una richiesta in tal senso con le stesse modalità sopra previste ad una casella di posta appositamente predisposta dal fornitore di servizi.
Trascorsi trenta giorni dalla suddetta sospensione, il gestore provvede al ripristino dell'identità precedentemente sospesa qualora non riceva copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione. In caso contrario l'identità digitale viene ripristinata. Nel caso previsto dal punto 5, l'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento e a titolo gratuito, la sospensione o la revoca della propria identità digitale seguendo modalità analoghe a quelle previste dal precedente punto 4, ovvero attraverso:

a) richiesta al gestore inviata via PEC[2] alla seguente casella namirial.id@sicurezzapostale.it;
b) richiesta inviata alla casella namirial.id@namirialtsp.com tramite la casella di posta nota al gestore in formato elettronico e sottoscritta con firma digitale.

[1] La richiesta via PEC sarà perseguibile solo se l'utente abbia precedentemente provveduto a censire la propria casella di posta elettronica certificata all'interno del pannello di gestione dell'identità SPID.

[2] La richiesta via PEC sarà perseguibile solo se l'utente abbia precedentemente provveduto a censire la propria casella di posta elettronica certificata all'interno del pannello di gestione dell'identità SPID.

c) richiesta inviata alla casella namirial.id@namirialtsp.com, tramite casella di posta elettronica diversa da quella nota al gestore, allegando la scansione del modulo di richiesta di revoca o sospensione firmato e copia del documento d'identità

Nel caso di richiesta di sospensione, trascorsi 30 giorni dalla suddetta sospensione, Namirial provvede al ripristino dell'identità precedentemente sospesa qualora non pervenga con le modalità sopra indicate una richiesta di revoca.

La revoca di una identità digitale comporta conseguentemente la revoca delle relative credenziali.

Si precisa che Namirial conserva la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla revoca dell'identità digitale.

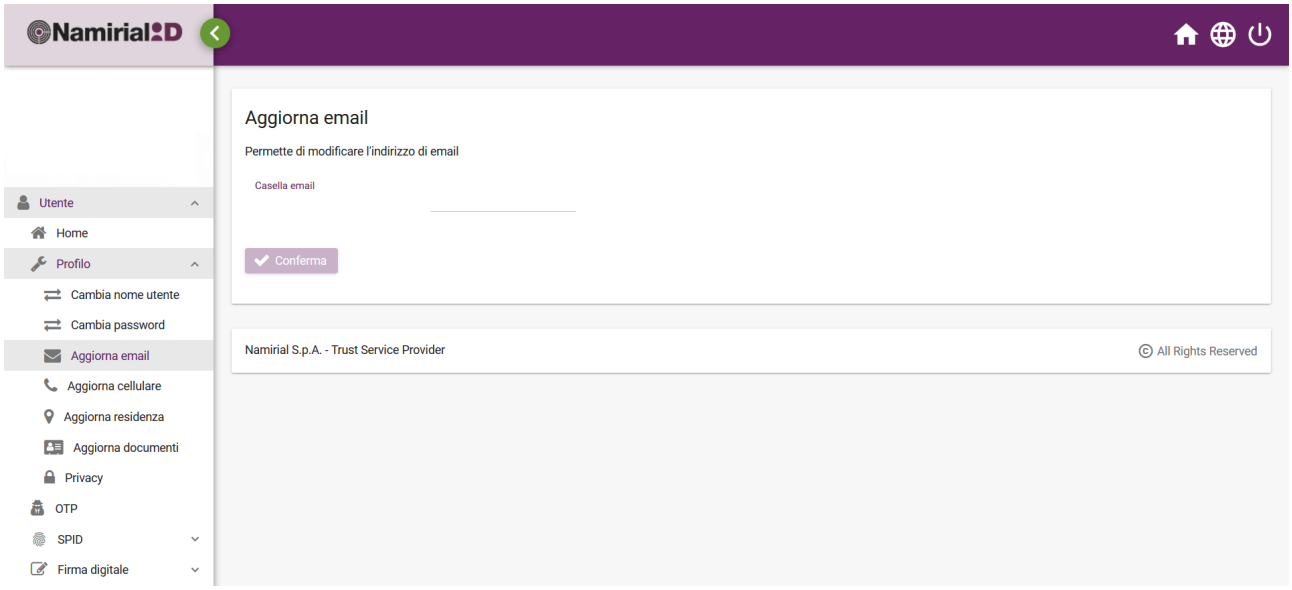
4.3 AGGIORNAMENTO DELLE INFORMAZIONI

Tramite il portale del Gestore, l'utente può procedere in autonomia all'aggiornamenti dei seguenti attributi relativi alla propria identità:

PERSONA FISICA
- Cambio del nome utente
- Cambio della password
- Aggiornare i propri attributi secondari (indirizzo e-mail, cellulare)
- Aggiornare i propri dati di residenza
- Aggiornare gli estremi del documento di riconoscimento e la sua scadenza
- Gestire i consensi al trattamento dei dati

PERSONA GIURIDICA
- Indirizzo sede legale
- CF o P.IVA (variazioni mutazioni societarie)
- legale rappresentante
- attributi secondari

L'accesso alle funzioni di aggiornamento dei dati relativi all'identità digitale è consentito solo con livello massimo tra quelli forniti dal Gestore. Tali funzioni seguono la stessa procedura e gli stessi criteri di autenticazione della Sospensione e Revoca. Ad esempio, nella figura che segue è riportata la funzione di modifica dell'indirizzo email a seguito dell'autenticazione di livello 2.
L'aggiornamento delle informazioni è comunicato all'utente utilizzando un attributo secondario funzionale alle comunicazioni (ad es. l'indirizzo di posta elettronica se non è stato modificato durante la sessione di aggiornamento).
Nel caso in cui sia modificato l'indirizzo di posta elettronica la comunicazione viene inviata al vecchio e nuovo indirizzo di posta.


NamirialID
Utente
Home
Profilo
Cambia nome utente
Cambia password
Aggiorna email
Aggiorna cellulare
Aggiorna residenza
Aggiorna documenti
Privacy
OTP
SPID
Firma digitale
Aggiorna email
Permette di modificare l'indirizzo di email
Casella email
Conferma
Namirial S.p.A. - Trust Service Provider
All Rights Reserved

4.4 GESTIONE CREDENZIALI

4.4.1 CONSERVAZIONE E CURA DELLE CREDENZIALI

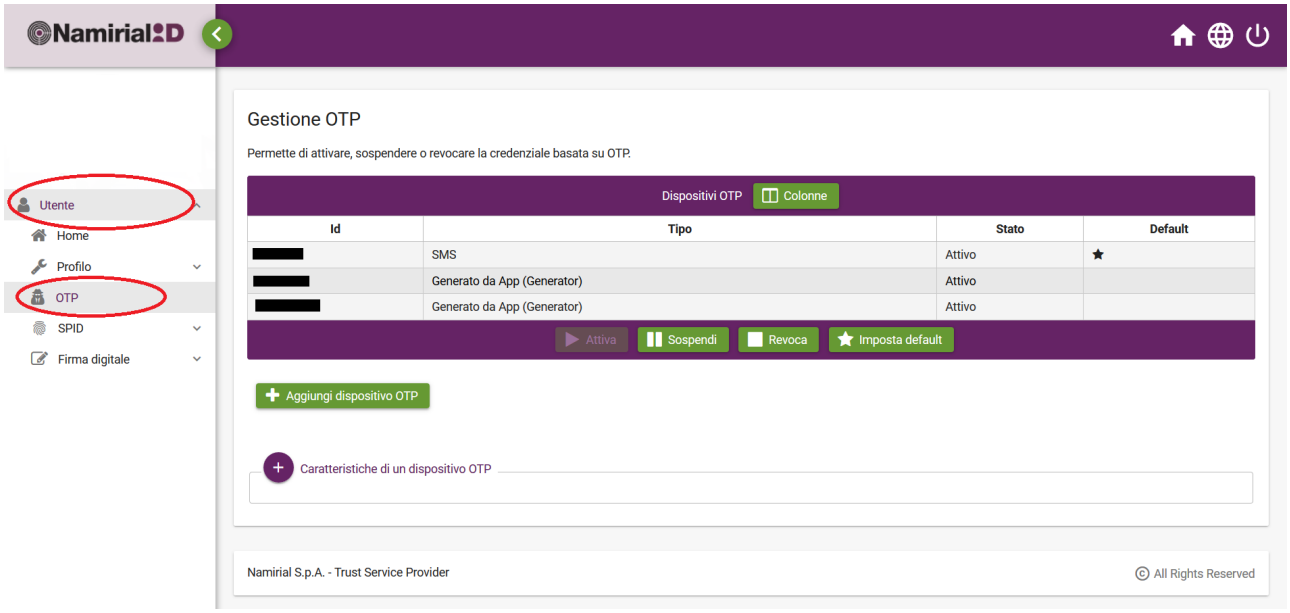
L'utente titolare dell'identità SPID è tenuto ad adottare tutti gli accorgimenti e buone pratiche, anche tecniche, idonee a custodire e utilizzare le credenziali con la diligenza del buon padre di famiglia.

Tra i principali accorgimenti da seguire ricadono:

- conservare con la massima segretezza la propria password e altri codici personali ricevuti dal Gestore
- non lasciare incustoditi i dispostivi personali associati all'identità SPID (es. cellulare)
- non alterare la configurazione hardware e/o software dei dispositivi personali associati all'identità SPID, es: jailbreak, root etc..
- comunicare tempestivamente il furto o lo smarrimento dei dispositivi personali
- comunicare tempestivamente eventuali accessi SPID inattesi comunicati attraverso il meccanismo di notifica via email
- verificare l'autenticità delle comunicazioni ricevute dal Gestore o presunte tali (cfr §6)

4.4.2 SOSPENSIONE E REVOCA DELLE CREDENZIALI

L'utente che intende **Sospendere** o **Revocare** le proprie credenziali SPID, può svolgere l'operazione all'interno della stessa area di gestione dell'Identità (§4), tramite l'apposita sezione "OTP" presente nel menù "Utente". La funzione di sospensione e revoca delle credenziali è accessibile tramite autenticazione di Livello 2 (quindi utilizzando il secondo fattore di autenticazione), ovvero con il codice di emergenza ricevuto al momento del rilascio dell'identità.



Sempre nella stessa sezione, l'utente può fare richiesta di una nuova credenziale OTP in sostituzione, ad esempio, di una revocata.

Oltre ai meccanismi disponibili da Area Web, così come previsto dal Regolamento [VIII], sono rese disponibili le seguenti modalità di inoltro delle richieste di Revoca e Sospensione delle credenziali SPID:

a) richiesta al gestore inviata via PEC alla seguente casella namirial.id@sicurezzapostale.it;
b) richiesta inviata alla casella namirial.id@namirialtsp.com tramite la casella di posta nota al gestore in formato elettronico e sottoscritta con firma digitale o elettronica;
   A titolo esemplificativo, nel caso di firma elettronica, è possibile inviare un'email al Gestore allegando la scansione del modulo di richiesta di revoca o sospensione firmato e copia del documento d'identità

A titolo informativo si ricorda che, ai sensi della normativa vigente, il gestore revoca la credenziale nei seguenti casi:

- smarrimento, furto o altri danni (con formale denuncia presentata all'autorità giudiziaria)
- utilizzo per scopi non autorizzativi, abusivi o fraudolenti da parte di terzi soggetti
- emissione di una nuova credenziale in sostituzione di una già in possesso dall'utente oppure di una credenziale scaduta

La revoca delle credenziali corrisponde alla cancellazione logica dell'identità digitale ed annulla definitivamente la validità delle credenziali.

L'operazione di revoca deve essere confermata entro un massimo di 30 giorni a seguito della data di richiesta della sospensione, altrimenti ne consegue la riattivazione automatica dell'identità digitale.
Nel caso specifico di credenziali contenute su dispositivo fisico – oltre alla revoca delle credenziali – è prevista anche la distruzione fisica dello stesso dispositivo.
A seguito della conferma dell'operazione di revoca – il gestore dell'identità digitale (IDP) adotta meccanismi in base ai quali comunica la causa e la data di revoca prevista all'utente, tramite messaggi di avviso (ripetuti ad intervalli di 90, 30, 10 giorni ed il giorno precedente alla revoca) all'indirizzo di posta ed al recapito telefonico registrato in fase di registrazione. La revoca di una identità digitale comporta la revoca delle relative credenziali.

La sospensione delle credenziali rappresenta un temporaneo inutilizzo e precede la possibile revoca delle credenziali. A seguito della richiesta da parte dell'utente, il Service Provider provvede alla sospensione dell'identità digitale per un massimo di 30 giorni tenendo informato lo stesso richiedente.
Il richiedente riceve immediatamente un'email con la conferma dell'avvenuta sospensione.
Durante tale arco temporale il richiedente può:

1. decidere di annullare la richiesta di sospensione
2. formalizzare la richiesta di sospensione

Nel primo caso l'identità digitale viene ripristinata, mentre nel secondo caso viene successivamente revocata. Qualora il richiedente non avanzi nessuna azione durante tale arco temporale l'identità digitale sarà automaticamente ripristinata dopo scaduto il periodo di 30 giorni dalla data della richiesta.

Si precisa che Namirial conserva la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla revoca dell'identità digitale.

5 SCADENZA E RINNOVO DELLE CREDENZIALI SPID

Alcune tipologie di credenziali prevedono una scadenza d'uso temporale, pertanto il Gestore dell'Identità Digitale (IdP) si occupa di fornire una nuova credenziale da consegnare all'utente.

5.1 SCADENZA

La scadenza delle credenziali comporta l'emissione della nuova credenziale da parte del Gestore dell'Identità Digitale (IdP), dietro esplicita richiesta dell'utente. A seguito del rinnovo della credenziale viene eseguita automaticamente la revoca della vecchia credenziale.
In prossimità della scadenza, il Gestore adotta meccanismi in base ai quali comunica all'utente, tramite messaggi di avviso (ripetuti ad intervalli di 90, 30, 10 giorni ed il giorno precedente alla scadenza) all'indirizzo di posta ed al recapito telefonico forniti entrambi in fase di registrazione.

5.2 RINNOVO

Il rinnovo delle credenziali implica che il Gestore dell'Identità Digitale (IdP) provveda a:

- creare una nuova credenziale da consegnare all'utente in sostituzione della credenziale scaduta;
- creare una nuova credenziale da consegnare all'utente in sostituzione della credenziale con causale guasto oppure upgrade tecnologico.

Il Gestore dell'identità digitale (IDP) – nel primo caso su richiesta del cliente e nel secondo caso su sua iniziativa – emette la nuova credenziale e revoca in automatico la credenziale precedente.

6 COMUNICAZIONI AGLI UTENTI

Gli utenti sono pregati di prestare particolare attenzione alle comunicazioni ricevute via email. In particolare, con l'intento di mitigare attacchi mirati al furto delle credenziali tramite e-mail contraffatte (Phishing), informiamo che per nessuna ragione il Gestore Namirial S.p.A. invia e-mail contenenti link diretti a risorse e/o contenenti allegati diversi da pdf statici.
Tutte le comunicazioni inviate da Namirial S.p.A. provengono o dal dominio @namirial.com o dalla seguente casella: namirial.id@namirialtsp.com e recano il logo del Gestore. Tale indirizzo può essere anche utilizzato per le comunicazioni che gli utenti intendono inviare al Gestore.

Nel caso in cui l'utente riceva comunicazioni sospette e/o presumibilmente contraffatte è invitato a segnalarlo tempestivamente al gestore affinché possano essere intraprese le relative azioni di notifica alle autorità competenti.