Namirial ID

SPID – Guida utente

Categoria	**SPID**	Codice Documento	**NAM-SPID-GU**	**Namirial S.p.A.**
Redatto da	**Simone Baldini**	Nota di riservatezza	**Documento Pubblico**	Il Legale Rappresentante
Verificato da	**Giuseppe Benedetti**	Versione	**1.3**	**Davide Ceccucci**
Approvato da	**Davide Ceccucci**	Data di emissione	**04/07/2017**	CECCUCCI DAV 2017.07.13 11:45:45 CN=CECCUCCI DAVIDE C=IT O=NON PRESENTE 2.5.4.4=CECCUCCI 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	**1.0**
Data	01/03/2017
Motivazione	Prima emissione del documento.
Modifiche	---

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

VERSIONE	**1.2**
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	**1.3**
Data	04/07/2017
Motivazione	Quarta emissione del documento.
Modifiche	• Aggiornato nome servizio SPID • Aggiornati link siti web e indirizzi email

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]	Decreto Legislativo (DLGS 196) 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n. 123 della Gazzetta Ufficiale n. 174, 29 luglio 2003
[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'identita' 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 9001:2008 – 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, le cautele che l'utente deve adottare per la conservazione e 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:

8. IdP – Identity Provider o Gestore dell'identità digitale: soggetto accreditato da AgID con finalità di creazione e gestione delle identità.
9. SP – Service Provider o Fornitore di servizi: soggetto, sia pubblico che privato, che eroga dei servizi dai propri siti internet utilizzando come modalità di accesso le credenziali SPID.
10. 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 del presente Manuale Operativo. 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	Accettarsi che l'informazione sia accessibile esclusivamente a coloro che sono autorizzati all'accesso.
BCP	Best Current Practice (IETF)
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 "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).
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).
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).
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 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.
ICT	Information and Communications Technology
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 del tipologia di identità: soggetto fisico / soggetto giuridico	Richiesta/Registrazione
• Inserimento degli attributi secondari (Username, Email, Cellulare) • Inserimento dati anagrafici	Registrazione/identificazione
• Acquisizione documento di identità e Tessera Sanitaria in corso di validità ed 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 se, oltre ai dati anagrafici, un numero di telefonia mobile (necessario per ricevere le comunicazioni SMS), una casella email attiva, un documento di identità valido e la Tessera Sanitaria.
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.

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

2.1.1.1 PERSONA FISICA/GIURIDICA

La pima fase prevede la registrazione del tipo di identità richiesta:

- Persona Fisica
- Persona Giuridica

2.1.1.2 USERNAME E CONTATTI

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.

Possesso dell'email e del cellulare sono verificati nella fase di rilascio dell'identità. Per maggiori informazioni riferirsi al Manuale Operativo.

2.1.2 ANAGRAFICA

La fase, "**Anagrafica**", è destinata all'inserimento delle seguenti informazioni:

- **Sesso** – inserire il sesso Maschio / Femmina
- **Cognome** – inserire il cognome del registrante
- **Nome** – inserire il nome del registrante
- **Codice Fiscale** – inserire il codice fiscale
-
- **Data di nascita** – inserire la data di nascita nel formato gg/mm/aaaa
- **Provincia di nascita** – indicare la provincia di nascita
- **Comune di nascita** – indicare il comune di nascita
- **CAP di nascita** – valore del CAP del comune di nascita
- **Nazione di nascita** – valore data di nascita
- **Indirizzo di residenza** (via, civico, cap, comune, provincia)
- **PEC** inserire, se a disposizione dell'utente, una casella PEC

La pagina dell'anagrafica presenta un'ulteriore sezione nel caso che l'utente stia richiedendo un'identità SPID per persona giuridica. La sezione richiede l'inserimento delle seguenti informazioni:

- **denominazione/ragione sociale**
- **codice fiscale o P.IVA (se uguale al codice fiscale);**
- **sede legale**
- **visura camerale** attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società o atto notarile di procura legale complete di data di rilascio e validità dello stesso;

In questo caso i dati sopraindicati vengono associati con quelli del richiedente ('Anagrafica') e del documento (fase 'Documento'). Il richiedente deve corrispondere con il legale rappresentante ovvero con il rappresentante indicato nell'atto notarile.

Al termine della registrazione dei parametri di anagrafica è possibile passare alla fase successiva: "**Documento"**.

2.1.3 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
- **Ente emittente** – inserire l'ente che ha emesso il documento utilizzato
- **Scansione Documento** – caricare la scansione fronte-retro del documento di identità
- **Scansione Tessera Sanitaria** – caricare la scansione fronte-retro della Tessera Sanitaria

2.1.4 LIVELLO E TIPOLOGIA SPID

In questa fase è possibile scegliere il livello e la tipologia di credenziali:

- Livello: **L1/L2**
- Tipo credenziali: **OTP Virtuale/OTP SMS**

2.1.5 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

Terminata la selezione sopra, passare alla funzione successiva **Modalità di identificazione.**

2.1.6 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. De Visu
La procedura è gestita dall'operatore RAO che esegue l'identificazione del richiedente e gli fa sottoscrivere il modulo di adesione al servizio SPID.

2.1.7 NUMERO TELEFONICO

Un'altra fase molto importante per il rilascio dell'identità SPID è la verifica del numero di cellulare registrato. Questa informazione, come anche l'email, sarà usata dal Gestore per inviare comunicazioni utili alla corretta gestione dell'identità SPID e delle relative credenziali.

Il numero di telefono, tramite apposita opzione, è verificato all'interno della fase di registrazione ed identificazione ovvero all'interno della fase di completamento descritta di seguito

2.1.8 COMPLETAMENTO

In questa fase viene inviata un'email alla casella registrata negli step precedenti.

L'email ha come oggetto "**Conferma Registrazione SPID**" e riporta un contenuto simile al seguente:

Namirial SPID

Gentile Utente,

Le comunichiamo la registrazione del Servizio Namirial ID abilitato a SPID, fornito da Namirial S.p.A., a cui hai aderito tramite accettazione, con firma elettronica, delle relative Condizioni contrattuali.

Il Servizio Namirial ID è stato profilato nella configurazione prevista dal livello di sicurezza da Te prescelto e indicato nel seguente riepilogo:

- LIVELLO 1 con nome utente e password
- LIVELLO 2 con APP Namirial Virutal OTP
- LIVELLO 2 con SMS su cellulare certificato

Per completare l'attivazione e confermare contestualmente email e cellulare, effettui il suo primo accesso presso un servizio abilitato o, in alternativa, presso le pagine del Gestore destinate al servizio https://portale.namirialtsp.com/private/user

Le credenziali temporanee da utilizzare per il completamento della richiesta sono:

Username: username

Password: ***

Alleghiamo alla presente il file che riporta le Condizioni contrattuali, l'Informativa privacy, il riepilogo dei Tuoi dati e dei consensi che hai rilasciato ai sensi del Codice privacy (D.Lgs. 196/2003), nonché le Tue dichiarazioni/accettazioni, rese anche ai sensi degli articoli 1341 e 1342 cod. civ.

Se hai scelto credenziali con associato strumento di autenticazione App Namirial Virtual OTP, dovrai configurare e attivare l'App mobile Namirial Virtual OTP scaricabile dagli store del tuo smaprtphone.

Il presente messaggio è generato automaticamente. Si prega di non rispondere a questa e-mail. *

Cordiali Saluti.

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, le condizioni generali di contratto e la guida utente.

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 email.

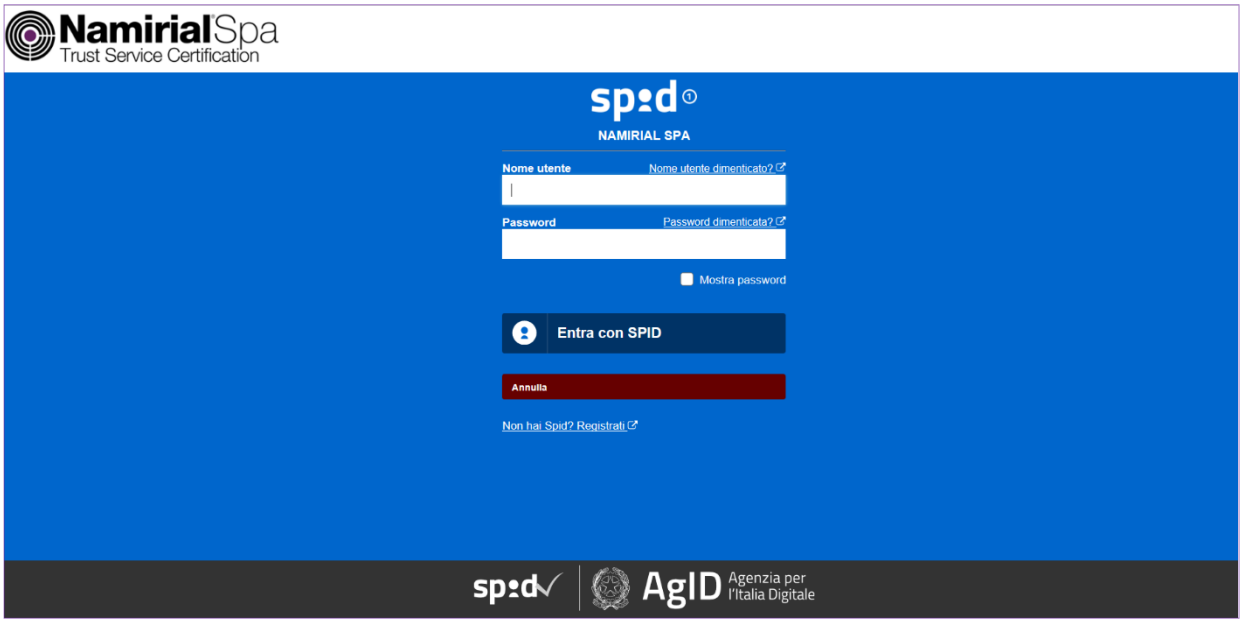


Figura 1 - Accesso SPID Namirial

All'interno di questa pagina viene chiesto l'inserimento del codice segreto temporaneo ricevuto per email.

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.

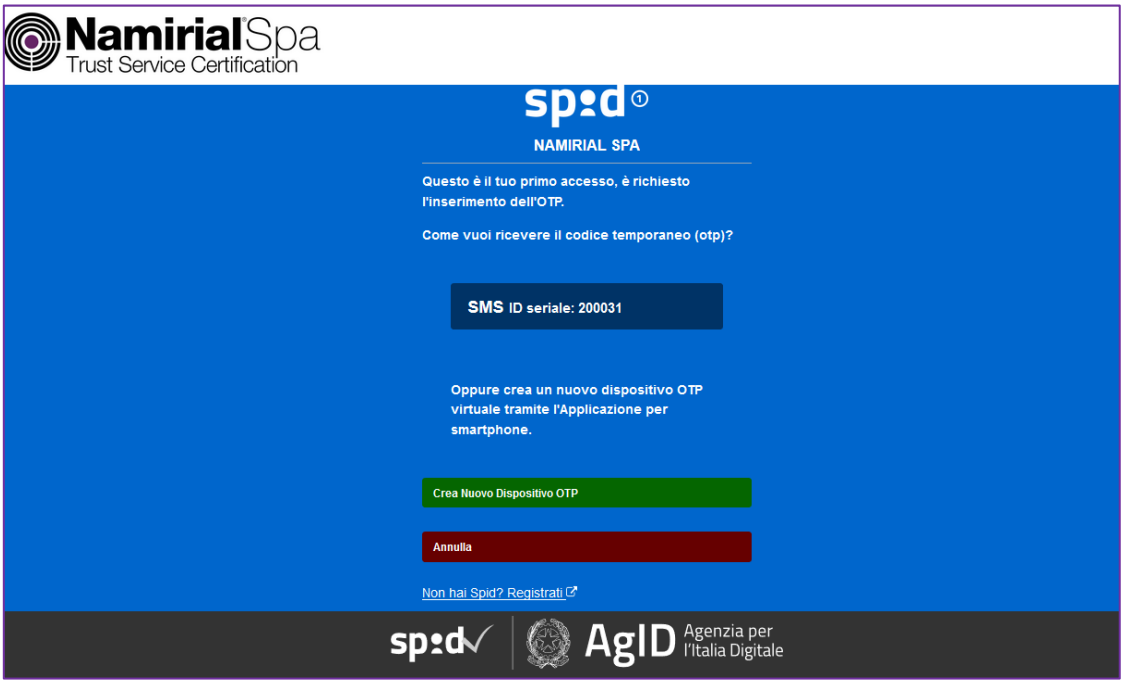


Figura 2 - Primo accesso SPID Namirial

L'utente è invitato a scegliere il tipo di credenziale da utilizzare per il primo accesso: **SMS** o **App OTP.**

SMS: Cliccando in questa funzione il sistema invia un codice SMS nel cellulare verificato. Il codice dovrà essere inserito nell'apposita maschera per completare l'attivazione e procedere con lo step successivo.

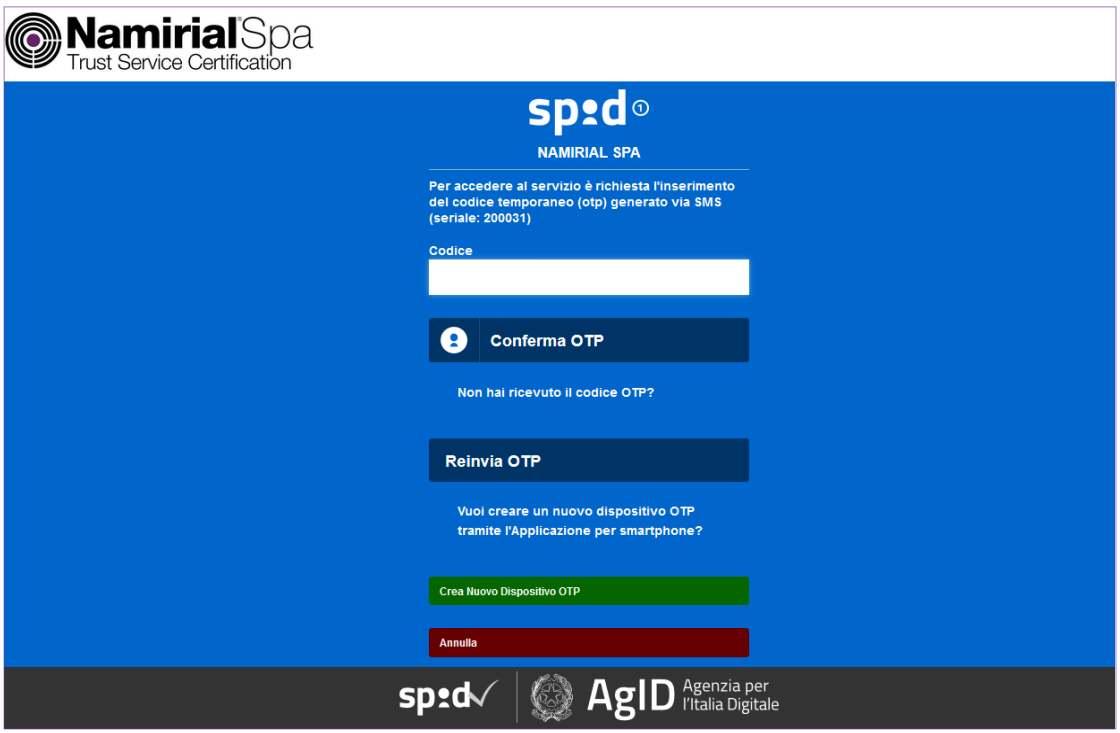


Figura 3 – Accesso con OTP su SMS

- **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.

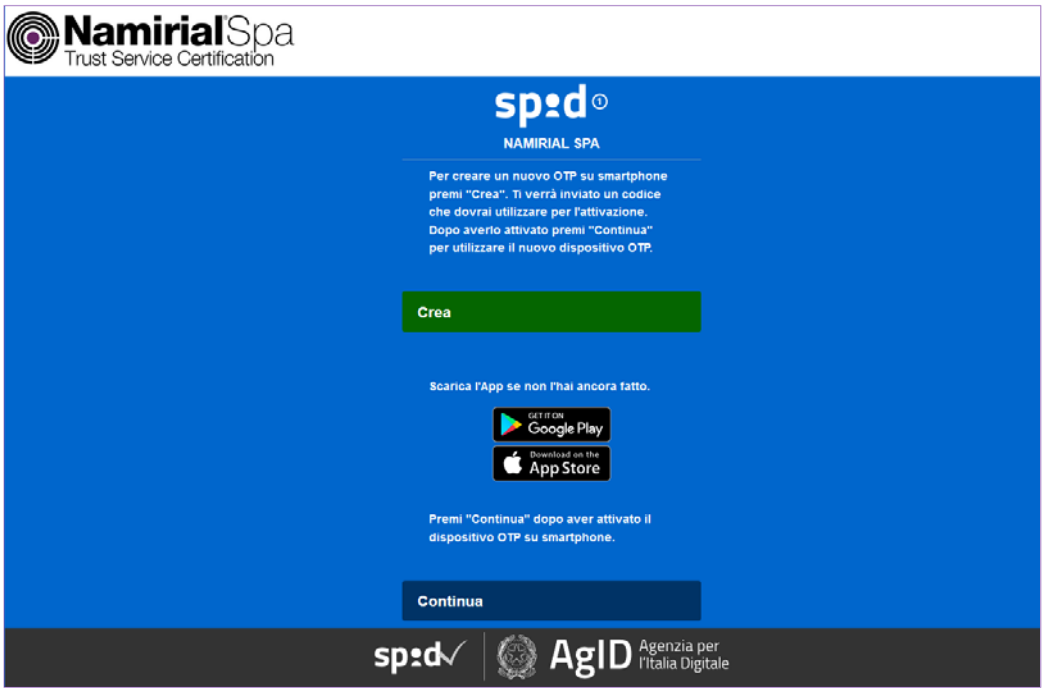


Figura 4 - Accesso con OTP su App

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

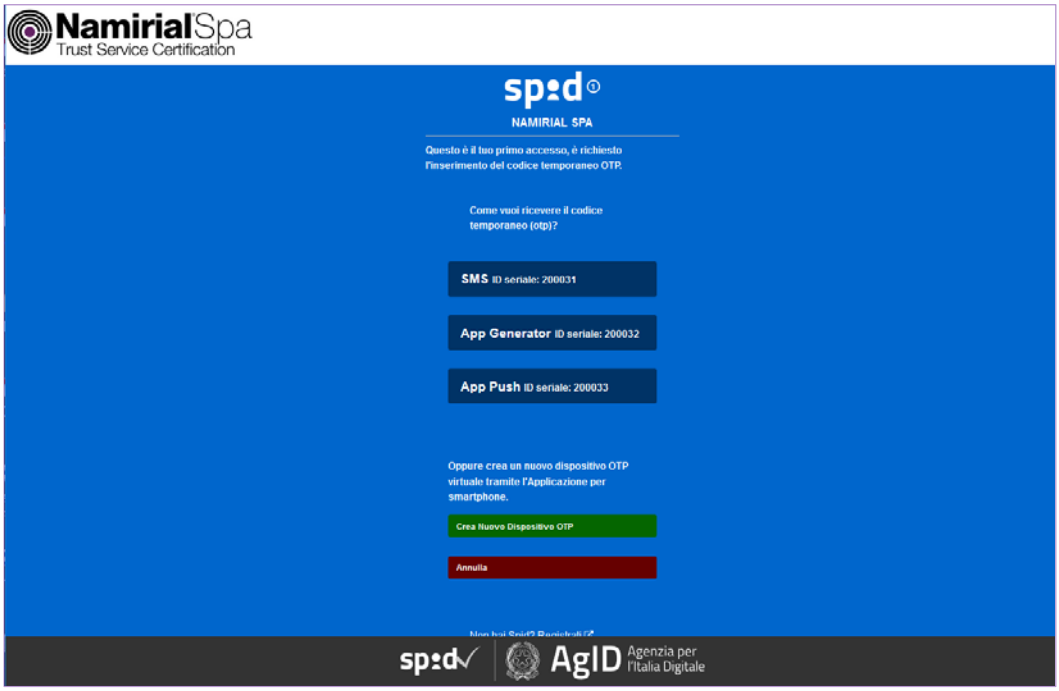
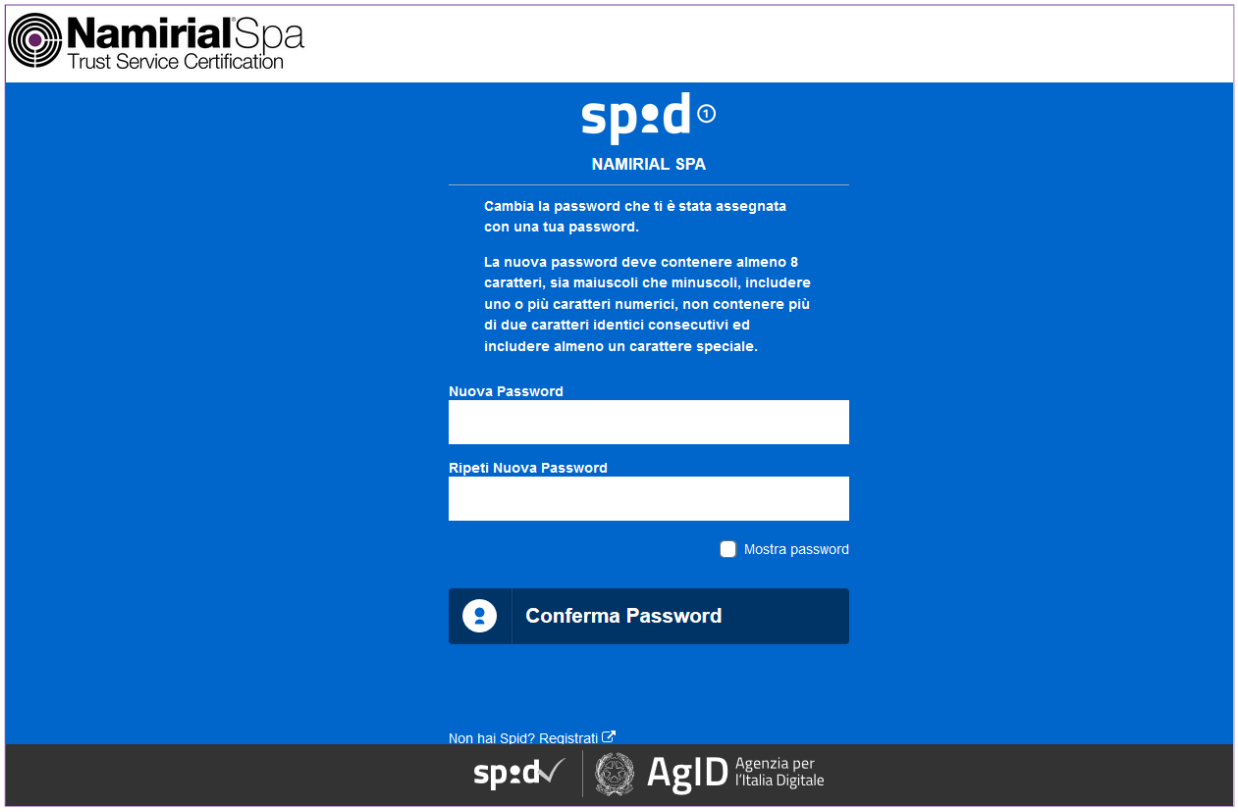


Figura 5 - Cambio Password SPID

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



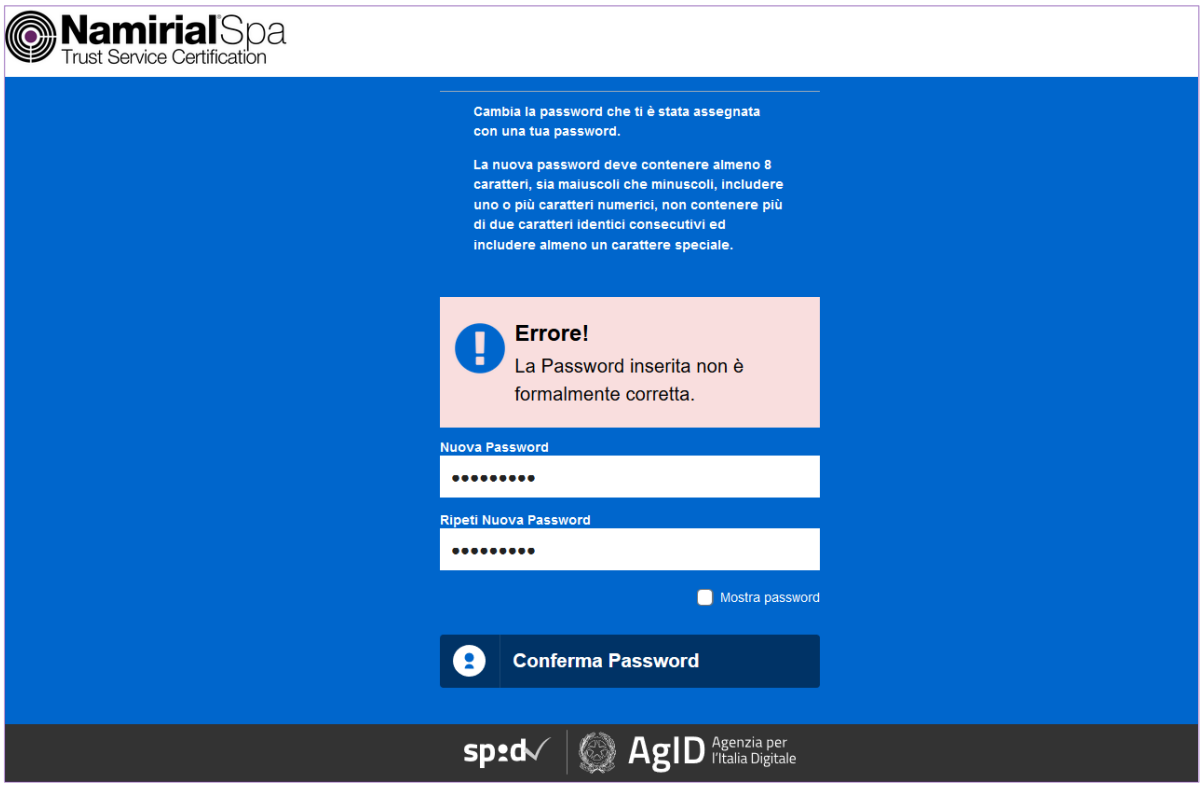
Nuova Password: inserire la password desiderata oppure ricorrere alla generazione casuale automatica tramite il link "Genera password random". In particolare, in relazione al tipo della password, la pagina raccomanda l'adozione di regole per ottenere password complesse e difficilmente attaccabili rispettando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

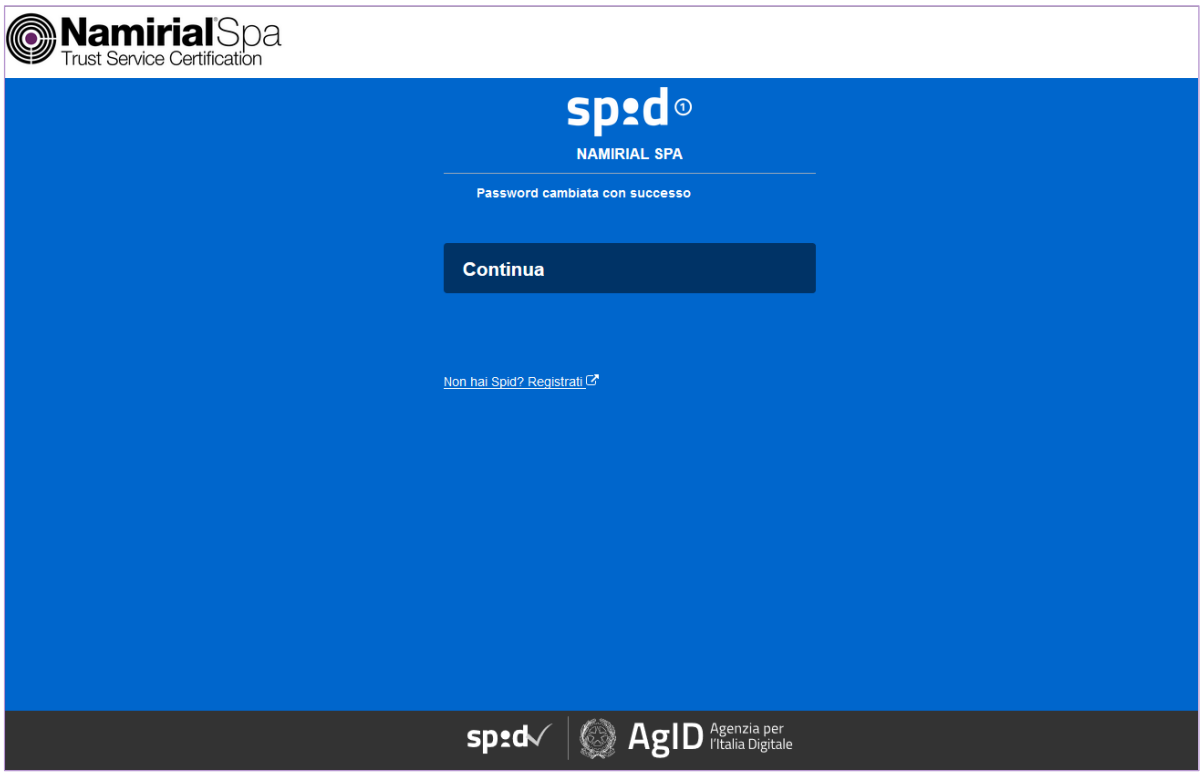
Si raccomanda poi di vietare l'uso di informazioni non segrete riconducibili all'utente (ad es. codice fiscale, patente auto, sigle documenti, date, includere nomi, account-Id ecc.).
Conferma la password: inserire nuovamente la password inserita nel precedente campo (doppia conferma)

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:

- modalità di identificazione e adesione al servizio (Sportello, etc..)
- tipologia di credenziali attivate
- codici 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.

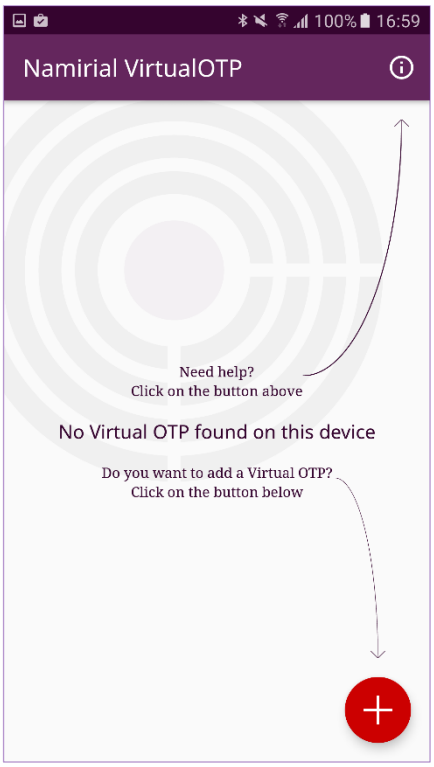
2.2.2 LIVELLO 2

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:

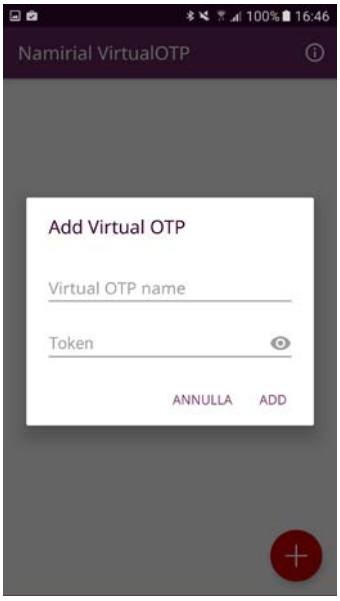
- OTP mobile
- OTP SMS

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

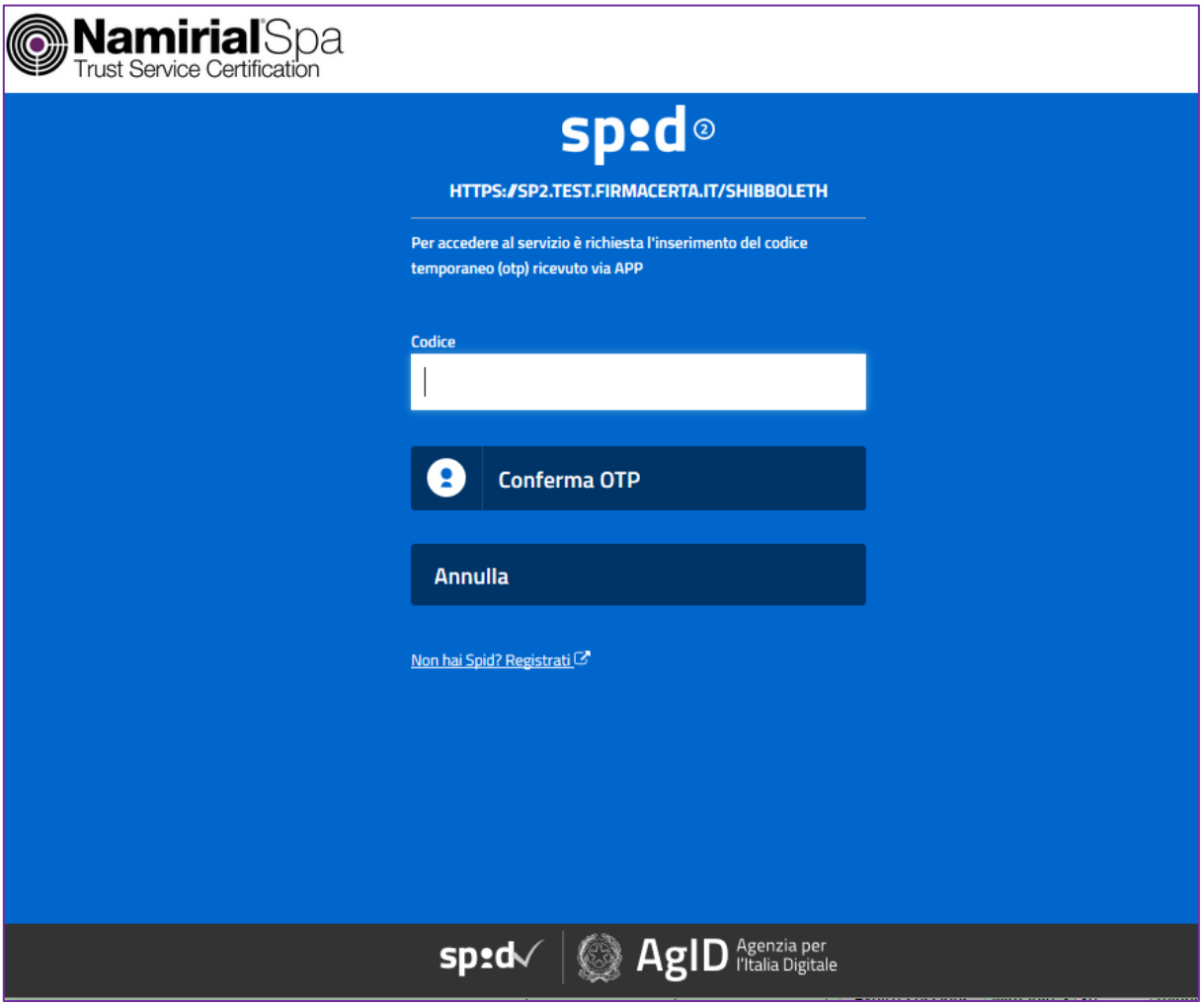


Figura 6 - Attivazione SPID L2 SMS

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 7 - 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

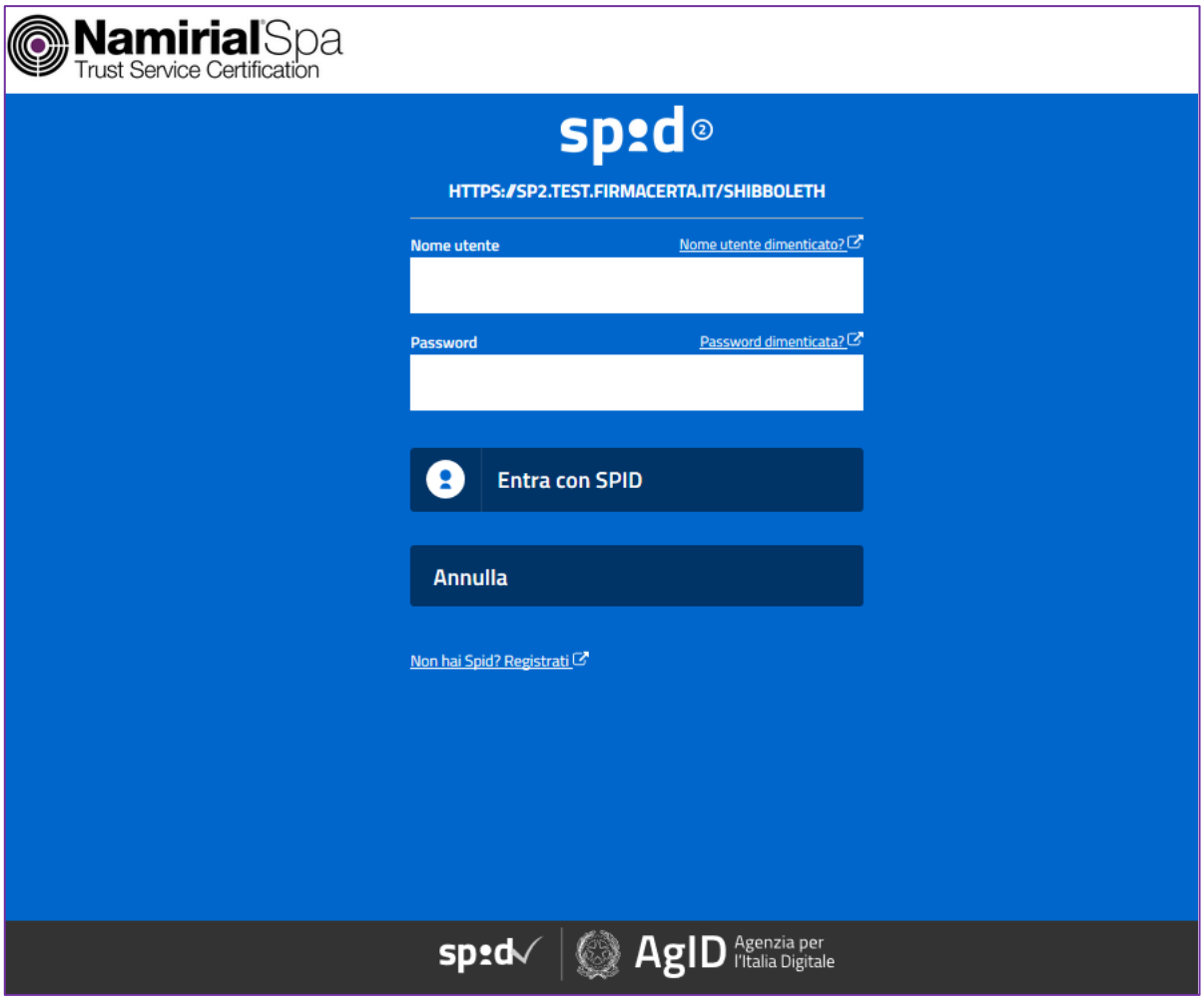


Figura 8 - Accesso SPID L1 Namirial

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:

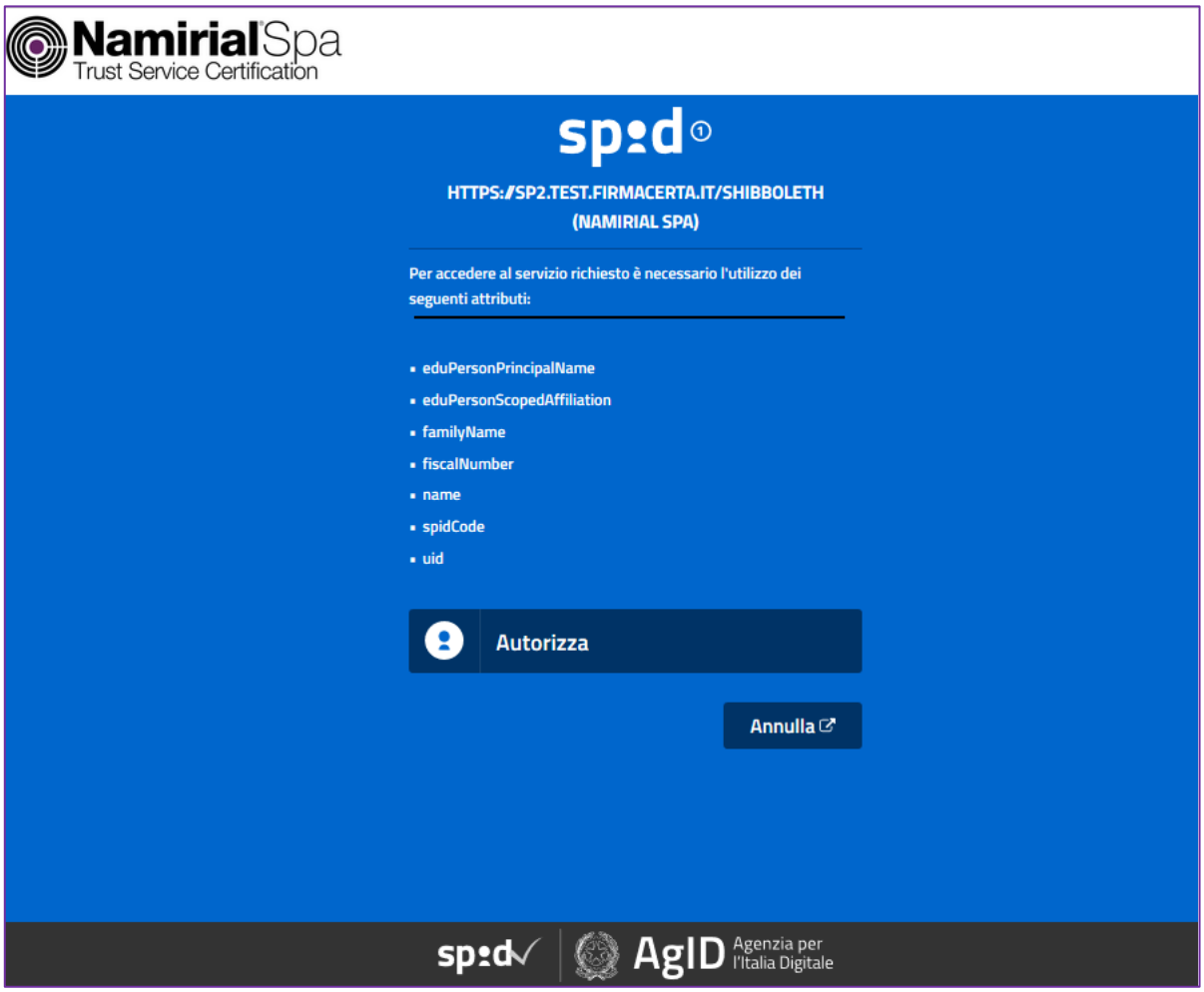


Figura 9 - Accesso SPID L1: Notifica attributi richiesti dal SP

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 10 - 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 11 - 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:

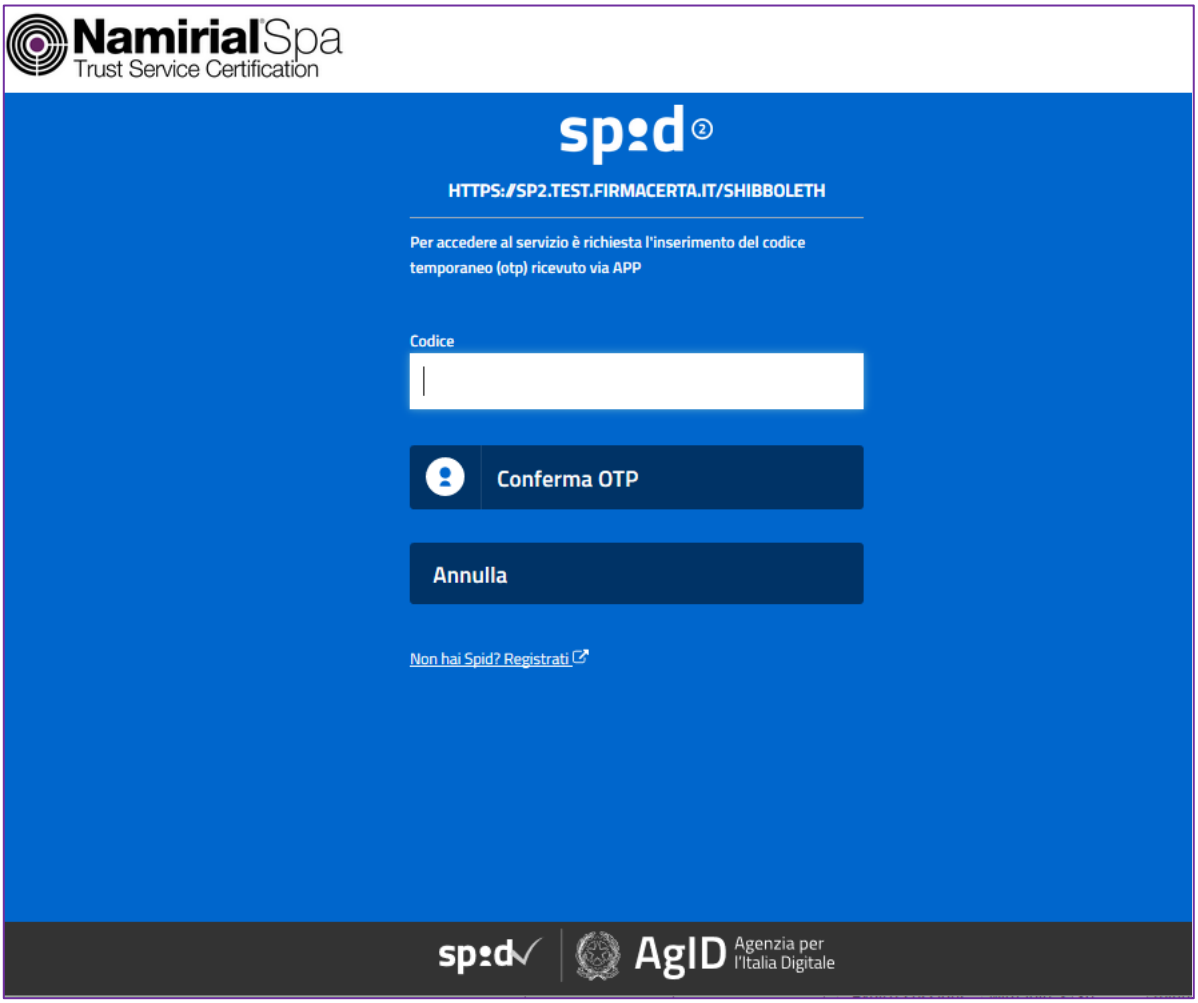


Figura 12 - Accesso L2 SPID Namirial: inserimento OTP

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.

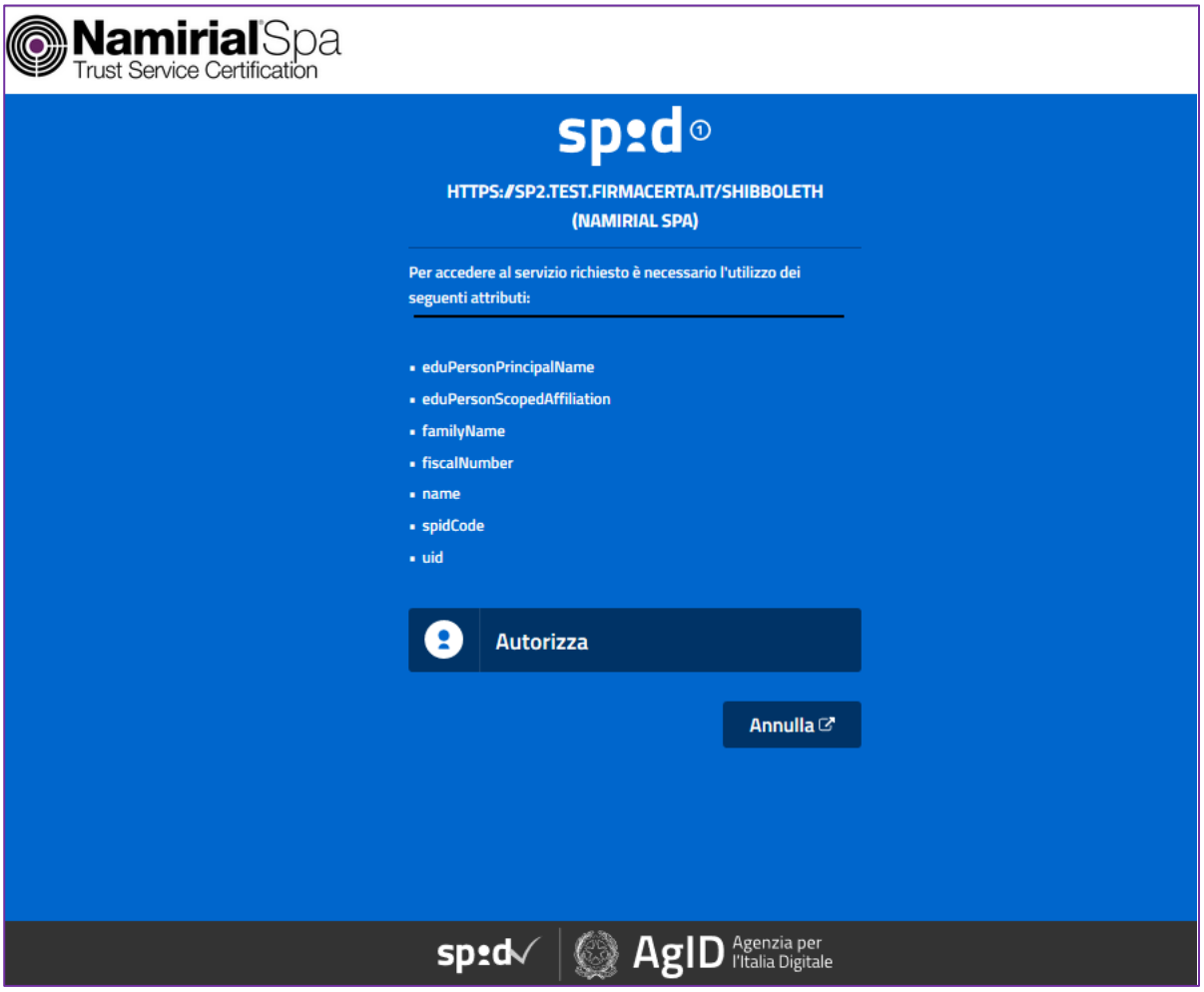


Figura 13 - Accesso SPID L2: Notifica attributi richiesti dal SP

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

.

4 GESTIONE DELL'IDENTITÀ SPID

Il Gestore mette a disposizione un'Area 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://portale.namirialtsp.com/private/user

Figura 14 - Area gestione SPID

All'interno dell'Area sono rese disponibili le funzioni descritte ai paragrafi successivi

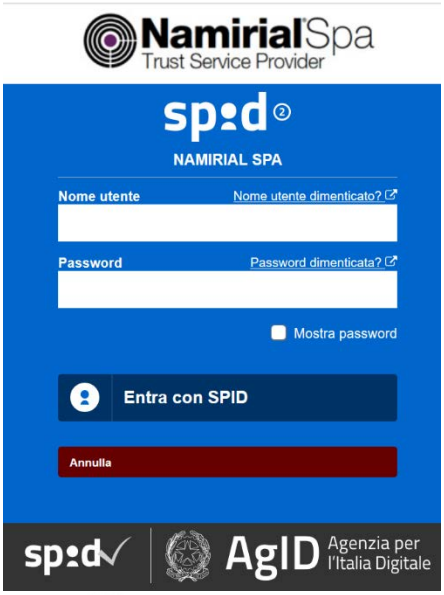
4.1 SOSPENSIONE E REVOCA DELL'IDENTITÀ DIGITALE

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

Figura 15 - SPID Namirial: Sospensione con Livello 2

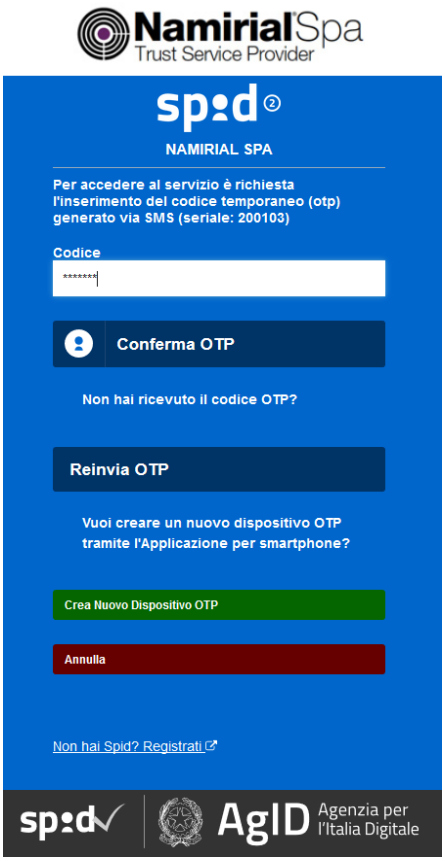
L'utente che intende procedere con la **Sospensione** dell'Identità attiva l'apposita funzione e viene rediretto sulle pagine dell'IdP che forzano l'autenticazione di livello 2.

L'utente inserisce user e password

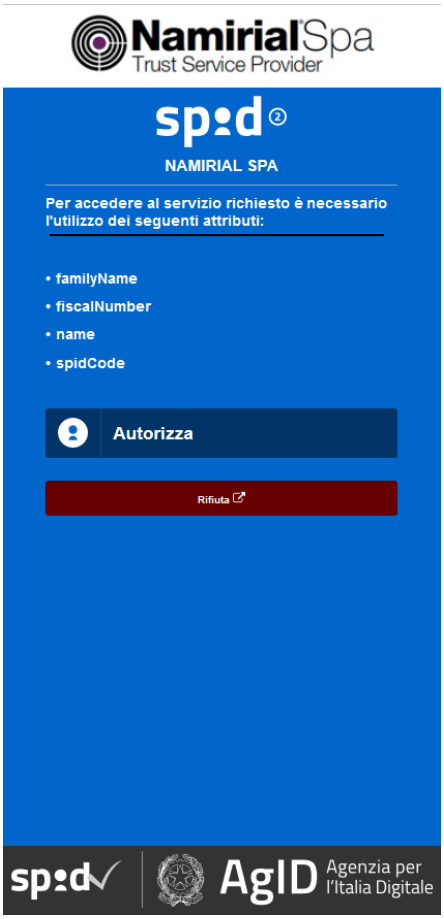


La pagina richiede quindi l'autenticazione di secondo livello per completare l'operazione.
In questo caso l'utente attiva la funzione di invio del codice OTP sul numero di cellulare censito ed attende l'arrivo del SMS on il codice OTP.

L'utente inserisce il codice ricevuto e procede alla sospensione dell'Identità



All'utente viene comunicata la richiesta di accesso ai dati dell'identità necessari all'espletamento della Sospensione



L'utente ottiene l'accesso alla funzione di Sospensione dell'identità e può procedere con l'operazione

La funzione di **Revoca** dell'Identità segue la stessa procedura e gli stessi criteri di autenticazione

Oltre al meccanismo disponibile da web portal, così come previsto dal Regolamento [VIII], sono rese disponibili le seguenti modalità di inoltro della richieste di Revoca e 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 al 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 al 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;

[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.

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

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.

4.2 AGGIORNAMENTO DELLE INFORMAZIONI

All'interno della pagina di Gestione delle identità, l'utente può procedere in autonomia all'aggiornamenti dei seguenti attributi relativi alla propria identità:

PERSONA FISICA
- Aggiornamento attributi secondari: **email** e **cell**
- Aggiornamento estremi documento di riconoscimento e scadenza

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

L'accesso alle funzioni **Gestione delle informazioni dell'Identità** 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 all'Area di Gestione dell'Identità.

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.


NamirialSpa
Trust Service Provider
Sospendi credenziali SPID
Attiva credenziali SPID
Revoca credenziali SPID
Resetta password SPID
Sblocca OTP
Cambio Password
Aggiorna E-mail
Aggiorna Cellulare
Aggiornamento dati personali
Attraverso questa sezione sarà possibile variare l'indirizzo e-mail associato alla sua identità SPID.
Attuale indirizzo e-mail
Nuovo indirizzo e-mail
Conferma nuova e-mail
Invia codice per E-mail
Invia e-mail
Codice di verifica
Salva

4.3 GESTIONE CREDENZIALI

4.3.1 CONSERVAZIONE E CURA DELLA CREDENZIALE

L'utente titolare dell'identità SPID è tenuto ad adottare tutti gli accorgimenti e buone pratiche, anche tecnici, idonei 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)

4.3.2 SOSPENSIONE E REVOCA DELLE CREDENZIALI

L'utente che intende **Revocare** o **Sospendere** le proprie credenziali SPID potrà volgere l'operazione all'interno della stessa area di gestione dell'Identità (§ 4), tramite l'apposita funzione.
La funzione di sospensione e revoca delle credenziali è accessibile tramite autenticazione effettuata con l'altra credenziale attiva, ovvero con il codice di emergenza fornito al momento del rilascio dell'identità.

All'interno dell'apposita funzione dell'Area l'utente può procedere ad effettuare le seguenti attività:

Funzione	Processo
Rinnovo e sostituzione	Tramite questa funzione l'utente può richiedere il rinnovo e la sostituzione delle proprie credenziali. **Livello 1:** L'utente viene reindirizzato all'interno del wizard per il cambio della password (vedi sotto). Seguendo la procedura verrà assegnata la nuova password con durata pari a 180 gg.
Sblocco OTP	Nel caso in cui l'utente abbia inavvertitamente bloccato la credenziale OTP questa funzione permette lo sbloccotramite un wizard che prevede l'inserimento dello username, della password e del codice di emergenza ricevuto al momento dell'attivazione
Reset / Cambio password	Questa funzione permette di resettare la password nel caso in cui sia stata dimenticata ovvero cambiarla nel caso in si sospetti che sia stata rivelata. Per il **Cambio** password l'utente seguirà un wizard simile a quello adottato da altri portali in cui viene richiesta la conoscenza della precedente password e quindi l'inserimento e conferma della nuova. Per il **Reset** della password l'utente seguirà un wizard simile in cui, al posto della precedente password (si presume non nota), verrà inserito un codice OTP valido ovvero il codice di emergenza ricevuto al momento dell'attivazione.
Revoca / Sospensione	La **Revoca** o **Sospensione** della credenziale segue lo stesso flusso dell'analoga funzione per l'identità digitale con la differenza che viene richiesta l'autenticazione

	dell'utente tramite l'altra credenziale ancora valida ovvero con il codice di emergenza ricevuto al momento dell'attivazione.

Tabella 4 - Funzioni Revoca o Sospensione Credenziale Narmirial

Oltre ai meccanismi disponibili da Area Web, così come previsto dal Regolamento [VIII], sono rese disponibili le seguenti modalità di inoltro della 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 DELLA CREDENZIALE SPID

Alcune tipologie di credenziali prevedono una scadenza d'uso temporale, pertanto il Gestore (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 dell'identità digitale (IDP) 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 registrato.

5.2 RINNOVO

Il rinnovo delle credenziali implica che il Gestore (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 email contraffatte (Phishing), informiamo che per nessuna ragione il Gestore Narmirial invia email contenenti link diretti a risorse o contenenti allegati diversi da pdf statici.

Tutte le comunicazioni inviate da Namirial provengono dalla seguente casella: namirial.id@namirialtsp.com e recano il logo del Gestore. Tale indirizzo può essere anche utilizzato per comunicazione che gli utenti intendono inviare al Gestore.

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