



# SPID user experience

## **Linee guida per la progettazione dell'esperienza e delle interfacce del servizio di identità digitale nazionale**

Questo 5 SPID.

Si richiede agli Identity Provider e ai Service Provider di seguire tali indicazioni e di avvalersi liberamente dei materiali già a disposizione nei repository che troverete linkati alla fine di questo documento.

Il documento sostituisce il documento [Note tecniche sulle interfacce e sulle Informazioni Idp/Sp](#), emanato il 02/2015, che viene abrogato contestualmente alla pubblicazione del presente documento.

L'adeguamento alle nuove linee guida dovrà essere finalizzato entro il *<data da definire>*.

## **INDICE DEL DOCUMENTO**

<b>Come leggere il documento</b>	<b>4</b>
----------------------------------	----------

## **01 Il Sistema SPID**

<b>1.1 Descrizione Generale del Servizio</b>	<b>5</b>
<b>1.2 Credenziali e Livelli</b>	<b>6</b>
1.2.1 Livello 1 - Nome utente e password	6
1.2.2 Livello 2 - Codice temporaneo, fattore biometrico o PIN	7
1.2.3 Livello 3 - Dispositivo di accesso	8
<b>1.3 Ecosistema di SPID</b>	<b>8</b>
<b>1.4 Sessioni, Single Sign On e Passaggi di Livello</b>	<b>9</b>
1.4.1 SPID Livello 1 (LoA2)	9
1.4.2 SPID Livello 2 (LoA 3)	10
1.4.3 SPID Livello 3 (LoA 3)	10
1.4.4 SPID Passaggio di livello all'interno dello stesso servizio	10

## **02 Il Brand SPID**

<b>2.1 Logo, pulsanti e loro utilizzo</b>	<b>12</b>
2.1.1 Logo	12
2.1.2 Declinazione del logo	13
2.1.3 Pulsante "Entra con SPID"	16
<b>2.2 Tone of Voice e Lingua</b>	<b>19</b>
<b>2.3 Lingue ufficiali</b>	<b>21</b>
<b>2.4 Terminologia di SPID</b>	<b>21</b>

## 03 User experience, Template e Flussi

<b>3.1 Introduzione</b>	<b>23</b>
<b>3.2 Flussi e Template per gli Identity Provider</b>	<b>23</b>
3.2.1 Pagina Informativa	23
3.2.2 Flusso di Registrazione	25
3.2.2.1 Selezione del tipo di SPID richiesto e del metodo di riconoscimento	26
3.2.2.2 Log-in con un eventuale account già esistente / Inserimento dati anagrafici e di contatto	26
3.2.2.3 Visualizzazione delle condizioni generali di servizio e della privacy	27
3.2.2.4 Scelta delle credenziali per l'account SPID	27
3.2.2.5 Riconoscimento	28
3.2.3 Flussi di Accesso	29
Primo livello	30
Secondo livello;	32
Terzo livello.	32
3.2.4 Pagina di Gestione dell'Identità SPID	33
<b>3.3 Flussi per i Service Provider</b>	<b>35</b>
3.3.1 Pulsante di Accesso	35
3.3.1.1 Posizionamento del pulsante di accesso	35
3.3.1.2 Label del pulsante di accesso	37
3.3.1.3 Utente già loggato	37
3.3.2 Pagina di Disambiguazione	38
3.3.2.2 Utente non registrato	41
3.3.3 Il Pulsante Entra con SPID	42
3.3.3.1 Applicazioni mobili e webview	42
3.3.3.2 Caso di Identity Provider che usa il proprio SPID (in maniera esclusiva rispetto agli SPID di altri Identity Provider) per far accedere ai propri servizi.	43
3.3.3.3 Quando il Service Provider ha bisogno di dati aggiuntivi	44
3.3.2 Procedure di Registrazione Assistita e Riutilizzo delle Identità Pregresse	44

3.3.3 Deleghe	47
<b>3.4 Errori e Notifiche di utilizzo</b>	<b>49</b>
Errori	50
Notifiche (inviate dall'Identity Provider)	53
<b>04 Risorse, Asset e Materiali</b>	
<b>4.1 Sito Ufficiale di SPID</b>	<b>55</b>
<b>4.2 Developers Italia</b>	<b>56</b>
<b>4.3 Sezione SPID AgID</b>	<b>56</b>
<b>4.4 Piano Triennale</b>	<b>56</b>
<b>4.5 CAD</b>	<b>57</b>

## Come leggere il documento

I contenuti di questo documento sono stati redatti dal Team per la Trasformazione Digitale con la collaborazione di AgID e definiscono lo standard qualitativo della user experience di SPID richiesto agli Identity e Service Provider.

Ogni contenuto è stato chiaramente caratterizzato come:

❖ **informativo**: gli Identity Provider e i Service Provider sono tenuti a conoscere questo tipo di contenuti e, dove riportato, possono utilizzare i contenuti all'interno delle loro properties digitali;

© **raccomandazione**: gli Identity Provider e i Service Provider sono tenuti a considerare questo tipo di contenuti come best-practice e ad implementare quanto descritto o un'alternativa che ne condivida obiettivi, caratteristiche e risultati;

👉 **normativo**: gli Identity Provider e i Service Provider sono tenuti a implementare quanto descritto nella forma descritta.

Il Team per la Trasformazione Digitale si rende disponibile per supportare gli Identity Provider e i Service Provider nell'analisi della propria esperienza utente e nel definirne eventuali evoluzioni.

# 01 Il Sistema SPID

## 1.1 Descrizione Generale del Servizio

❖ Questo paragrafo ha carattere informativo.

*Le informazioni qui presenti possono essere usate dai diversi attori per descrivere SPID sulle proprie properties digitali.*

SPID è il sistema pubblico di identità digitale nazionale, disponibile per i cittadini italiani che abbiano compiuto i 18 anni.

SPID permette di accedere a tutti i servizi online della Pubblica Amministrazione e di privati accreditati, con un'unica Identità Digitale (nome utente e password) ed è utilizzabile da computer, tablet e smartphone.

### Vantaggi per il cittadino

- Un solo set di credenziali, per tutti i servizi della Pubblica Amministrazione e dei privati accreditati;
- Maggiore sicurezza e privacy garantita: al contrario di altri sistemi diffusi di login, SPID garantisce che ogni servizio a cui il cittadino accede riceva sempre e solo le informazioni minime necessarie per la fornitura del servizio e che tali informazioni non vengano condivise con terze parti, se non esplicitamente comunicato e accettato dall'utente;
- Diffusione a livello europeo: da settembre 2018 l'identità SPID può essere utilizzata per accedere anche ai servizi della Pubblica Amministrazione di tutti i paesi membri dell'Unione Europea.

### Vantaggi per i Service Provider pubblici e privati

- Abbandono dei servizi di autenticazione proprietari, gestiti localmente, con un conseguente risparmio sui costi di manutenzione e di lavoro necessario per il rilascio di credenziali;
- Garanzia per chi eroga il servizio circa l'identificazione: la qualità dell'identificazione fornita da SPID è allineata alle specifiche eIDAS e garantisce anche la PA o il Service Provider privato durante l'erogazione di servizi.

## 1.2 Credenziali e Livelli

❖ Questo paragrafo ha carattere informativo.

SPID ha tre diversi livelli di identità, ciascuno dei quali assicura un diverso livello di sicurezza e permette di accedere a informazioni più o meno sensibili o di effettuare operazioni dispositive e di autenticazione.

I livelli di sicurezza di SPID sono riconducibili ai Levels of Assurance definiti dalla norma ISO / IEC 29115, che norma il grado di affidabilità all'interno dei processi che prevedono un'autenticazione. In generale un Level of Assurance fornisce la garanzia che l'entità che rivendica una particolare identità, è in effetti l'entità a cui tale identità è stata assegnata.

Pubbliche Amministrazioni e privati definiscono autonomamente il livello di sicurezza necessario per poter accedere ai propri servizi digitali. AgID, in collaborazione con le Regioni, ha emanato un avviso che contiene indicazioni sull'uso dei livelli in base alla tipologia dei servizi, consultabile sul [sito di AgID](#).

Di seguito riportiamo ulteriori dettagli che possono essere utili per effettuare una scelta in tal senso. In generale si richiede una valutazione attenta dei rischi associati al singolo servizio, per evitare richieste di autenticazione sovradimensionate per servizi "semplici" o sottodimensionate per servizi "sensibili".

### 1.2.1 Livello 1 - Nome utente e password

❖ Questo paragrafo ha carattere informativo.

Il primo livello di SPID consiste in nome utente e password del cittadino.

Il nome utente ad oggi può essere:

- un indirizzo e-mail;
- il codice fiscale;
- una stringa testuale (contenente lettere e/o numeri).

Il livello 1 corrisponde al Level of Assurance (LoA) 2 della norma ISO / IEC 29115. Con questo livello il cittadino può accedere ai servizi che richiedono una verifica sicura dell'identità, ma che non mostrano dati sensibili in prima battuta.

In generale si usa il livello 1 di SPID quando il rischio legato a un'autenticazione errata è moderato.

### 1.2.2 Livello 2 - Codice temporaneo, fattore biometrico o PIN

❖ Questo paragrafo ha carattere informativo.

Il livello 2 di SPID permette l'accesso ai servizi con nome utente e password, insieme a un codice temporaneo (*OTP*) che viene inviato all'utente via sms, email o che può essere generato tramite app mobile dedicata o strumenti analoghi.

Il livello 2 può anche essere utilizzato per confermare le operazioni dispositive previste da un servizio a cui l'utente ha acceduto con SPID di livello 1.

Corrisponde al Level of Assurance 3 e si usa quando il rischio relativo a un'autenticazione errata è medio-alto. Si usa per accedere a informazioni sensibili o per autorizzare operazioni dispositive associate a un rischio consistente (es. transazioni finanziarie, richiesta di cambio o sospensioni dell'identità, ecc.).

### App companion

© Questo paragrafo ha carattere di raccomandazione.

L'autenticazione attraverso app avviene attraverso un apposito codice PIN (qualcosa che sai), creato dall'utente al primo accesso. Per facilitare l'esperienza, soprattutto su dispositivi mobile, è possibile sostituire tale codice PIN con fattori biometrici (qualcosa che sei) come ad esempio un'impronta digitale.

Prima di poter utilizzare l'app come fattore di secondo livello, l'utente deve effettuare una procedura di first time use, accedendo con il nome utente e password di SPID e inserendo un codice di sicurezza che gli è stato fornito in uno dei modi riportati all'inizio del paragrafo o successivamente all'avvenuta registrazione a SPID. Una volta autenticato, l'utente può creare il suo PIN e/o abilitare l'utilizzo dei fattori biometrici (se permesso dalle caratteristiche del telefono utilizzato) da utilizzare in futuro come secondo fattore per l'accesso con SPID.

L'Identity Provider può anche fornire l'opzione di securizzazione dell'app con PIN o fattore biometrico, non obbligatoria, lasciando la scelta al cittadino.

Si rammenta che le app companion degli Identity Provider che forniscono l'identità digitale ai cittadini italiani residenti all'estero, devono essere rese disponibili anche sugli store stranieri.

### 1.2.3 Livello 3 - Dispositivo di accesso

❖ Questo paragrafo ha carattere informativo.

Il livello 3 di SPID permette l'accesso con strumenti forti di autenticazione, compliant al LoA4 e possono essere progettati e proposti direttamente dai diversi IdP.

Il livello 3 è equiparabile a una firma digitale e consente di accedere a informazioni altamente sensibili (es. risultato esami medici, volontà testamentarie) oppure di autenticare/autorizzare operazioni altamente sensibili (es. firma di contratti vincolanti).

## 1.3 Ecosistema di SPID

❖ Questo paragrafo ha carattere informativo.

L'identità SPID è rilasciata dai Gestori di Identità Digitale (Identity Provider), soggetti pubblici o privati accreditati da AgID che, nel rispetto delle regole emesse dall'Agenzia, forniscono le identità digitali e gestiscono l'autenticazione degli utenti.

Per ottenere un'identità SPID l'utente deve farne richiesta al gestore che preferisce e che più si adatta alle sue esigenze. Il gestore, dopo aver verificato i dati del richiedente, emette l'identità digitale rilasciando le credenziali all'utente.

Ogni gestore può scegliere tra [diverse modalità di riconoscimento](#) per verificare l'identità del cittadino. Qualunque sia il canale attraverso cui avviene il riconoscimento dell'utente, questo deve essere equivalente o superiore all'affidabilità di un riconoscimento *de visu*.


L'elenco dei gestori di identità digitale è riportata alla pagina:

<http://www.agid.gov.it/infrastrutture-architetture/spid/identity-provider-accreditati>



A questo [link](#) è possibile visualizzare il documento relativo agli obblighi dei Gestori e dei titolari di identità digitale SPID.

## 1.4 Sessioni, Single Sign On e Passaggi di Livello

 Questo paragrafo ha carattere normativo.

*Il paragrafo corregge gli argomenti trattati nell'avviso [Gestione delle sessioni SSO e Meccanismi di Single Logout](#) del 20/04/2016.*

Le sessioni di SPID presso l'Identity Provider iniziano nel momento in cui l'utente effettua un accesso di livello 1 (nome utente e password). La durata di tali sessioni è di 30 minuti.

Se lo stesso utente accede con SPID a un servizio A e, entro 30 minuti accede con SPID a un servizio B, o rientra nello stesso servizio A dopo essere precedentemente uscito, non dovrà reinserire le credenziali di livello 1.

Cliccando sul pulsante Entra con SPID, e selezionando l'Identity Provider, l'utente visualizza direttamente la pagina di conferma del passaggio dei dati dall'Identity Provider al servizio B. Nel passaggio da un servizio all'altro, è possibile richiedere un diverso set di attributi. Ad esempio, se il servizio A aveva richiesto codice fiscale, nome e cognome, il servizio B può chiedere il solo codice fiscale e l'indirizzo.

Di seguito sono riportate le tabelle che schematizzano il comportamento delle sessioni nel passaggio da un servizio A a un servizio B, all'interno della stessa sessione (quindi entro i 30 minuti dall'accesso al servizio A).

### 1.4.1 SPID Livello 1 (LoA2)

Livello Servizio A	Livello Servizio B	Flusso di autenticazione	Note
1	1	Nessuna ulteriore autenticazione richiesta	Single Sign On
1	2	Richiesta autenticazione di 2 livello (si veda <a href="#">paragrafo 1.2.2</a> )	
1	3	Richiesta autenticazione di 3 livello (specifica per Identity Provider)	

### 1.4.2 SPID Livello 2 (LoA 3)

Livello Servizio A	Livello Servizio B	Flusso di autenticazione	Note
2	1	Nessuna ulteriore autenticazione richiesta	Single Sign On

2	2	Richiesta autenticazione di 2 livello (si veda <a href="#">paragrafo 1.2.2</a> )	
2	3	Richiesta autenticazione di 3 livello (specifica per Identity Provider)	

### 1.4.3 SPID Livello 3 (LoA 3)

Livello Servizio A	Livello Servizio B	Flusso di autenticazione	Note
3	1	Nessuna ulteriore autenticazione richiesta	Single Sign On
3	2	Richiesta autenticazione di 2 livello (si veda <a href="#">paragrafo 1.2.2</a> )	
3	3	Richiesta autenticazione di 3 livello (specifica per Identity Provider)	


### 1.4.4 SPID Passaggio di livello all'interno dello stesso servizio

All'interno dello stesso servizio, l'utente può accedere con un livello di sicurezza X e poi doverlo aumentare per effettuare operazioni dispositive o per accedere a contenuti con un grado di sensibilità maggiore. In questi casi, il Service Provider effettua una chiamata all'Identity Provider, che richiede un accesso con un livello maggiore o uguale a quello utilizzato per accedere. Nel caso in cui l'accesso avvenga direttamente con livello 2 o 3, questo apre una sessione di livello 1 presso l'Identity Provider.

Livello iniziale	Livello operazione	Flusso di autenticazione	Note
1	2	Richiesta autenticazione di 2 livello (si veda <a href="#">paragrafo 1.2.2</a> )	
1	3	Richiesta autenticazione di 3 livello (specifica per Identity Provider)	
2	2	Richiesta autenticazione di 2 livello (si veda <a href="#">paragrafo 1.2.2</a> )	
2	3	Richiesta autenticazione di 3 livello (specifica per Identity Provider)	
3	3	Richiesta autenticazione di 3 livello (specifica per Identity Provider)	

# 02 Il Brand SPID

## 2.1 Logo, pulsanti e loro utilizzo

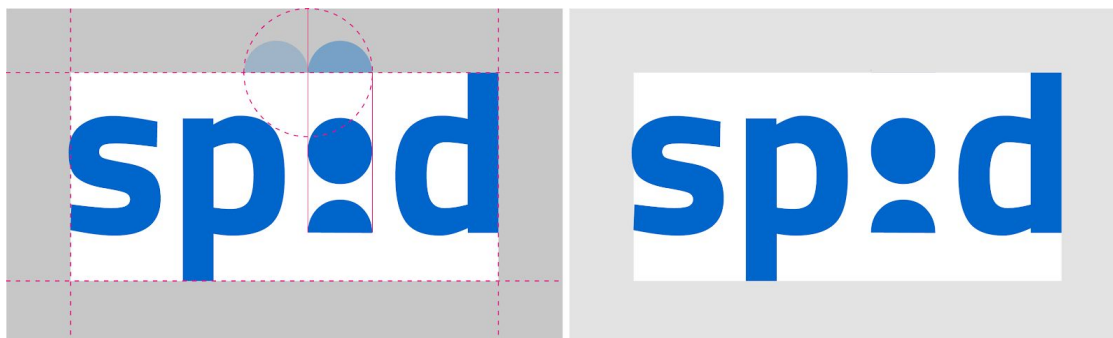
 Questo paragrafo ha carattere normativo.

### 2.1.1 Logo

Il logo SPID utilizza il font **Titillium Web Bold** e un elemento caratterizzante nel pittogramma dell'utente al posto della "i", come si vede nella griglia di costruzione. Il pittogramma è costituito da due cerchi: quello superiore è intero e rappresenta una testa, mentre quello inferiore è tagliato a metà e simula le spalle. I due cerchi raffigurano insieme una sorta di busto. Il colore identificativo è il **Blu Italia #0066CC** (RGB) – sia in versione positiva (blu su bianco), che nella versione negativa (bianco su blu) del logo – come da nuove linee guida di design.



L'area di rispetto del logo SPID corrisponde ad un cerchio, il cui diametro è la larghezza della "i" – questo spazio deve sempre essere rispettato per ogni lato descritto (sopra, sotto e in entrambi lati).



## Applicazioni d'uso

In generale il logo SPID deve essere sempre presente nelle pagine web o nelle schermate delle app mobile relative a:

- Descrizione del servizio SPID (Identity Provider) o del suo utilizzo presso il Service Provider – in pagina, in posizione prominente;
- Flussi di accesso tramite servizio SPID – all'interno dell'header;
- Flussi di registrazione al servizio SPID – all'interno dell'header;
- Flussi di recupero credenziali per l'utilizzo di SPID – in pagina, in posizione prominente.

Per avere un'idea più precisa sull'utilizzo del logo SPID in contesto, vedere il [capitolo 3](#).

### 2.1.2 Declinazione del logo



1.

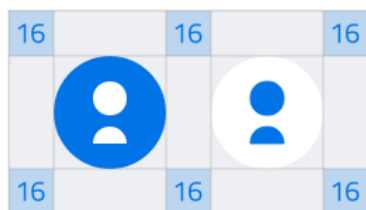


2.

Come si vede nell'immagine 1, il pittogramma dell'utente può essere inserito all'interno di un cerchio, diventando il **minimo elemento di Brand Identity** utilizzabile.

A sua volta, può essere utilizzato all'interno di un bottone che necessita di una brandizzazione, nella quale si vuole sottolineare la presenza di SPID, senza però indicarla in lettere – come per esempio accade nel bottone "Accedi" di un Service Provider (esempio fittizio nell'immagine 2). Infine, la versione mobile del bottone "Accedi" si definisce tramite il solo uso del pittogramma nel cerchio (maggiori dettagli nel paragrafo [Versione minimizzata del bottone brandizzato SPID](#)).

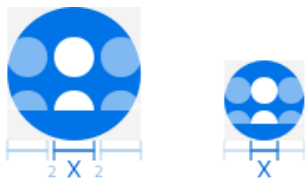
#### Visual del minimo elemento di brand



Il minimo elemento di brand rispetta le medesime regole del logo, per quanto riguarda codici cromatici e comportamento positivo/negativo: il colore primario è quindi il **Blu Italia**

**#0066CC** sempre accompagnato dal bianco. La sua area di rispetto consiste in un margine di **16px**, per ogni lato.

#### PROPORZIONI



>32px

<24px

La proporzione che determina la grandezza del pittogramma all'interno del cerchio contenitore corrisponde a 3x la larghezza dell'icona, con 2px di margine, nei bottoni con dimensioni superiori ai 32px. Invece, nei bottoni di grandezza 16-24px, è 3x la larghezza del pittogramma senza alcun margine.

#### DIMENSIONI UTILIZZABILI



Questo elemento può avere diverse dimensioni di diametro, purché siano multipli di 8. La **grandezza minima corrisponde a 16px**: non può essere utilizzato in dimensioni inferiori.

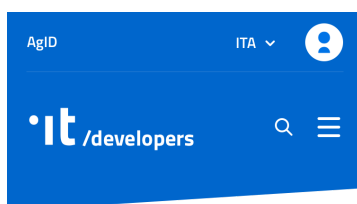
Se l'icona risiede all'interno dei bottoni deve avere le seguenti grandezze:

- **16px** se il bottone è **small** (altezza 40px),
- **24px** se il bottone è **medium** (altezza 48px)
- **32px** se il bottone è **large** (altezza 56px).

#### VERSIONE MINIMIZZATA DEL BOTTONE BRANDIZZATO SPID

Questo elemento è la versione minimizzata di un bottone brandizzato SPID all'interno di un **header mobile**. In questo caso la sua grandezza è di **40px**.

Se l'utente ha fatto login, al posto del pittogramma SPID, sarà possibile visualizzare al suo interno l'immagine di profilo, oppure l'iniziale del primo nome dell'utente (solo nel caso in cui non sia stata aggiunta un'immagine del profilo) la cui formattazione è Titillium Web Regular 20px, #0073E6.



Versione minimizzata pre-login

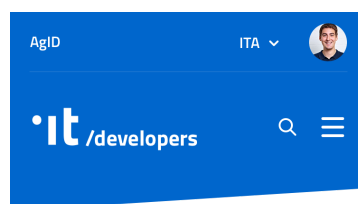
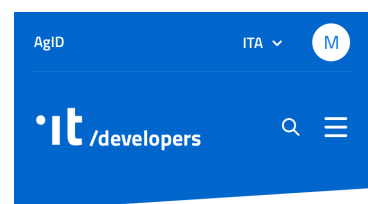


Foto / Post-login



Iniziale del nome / Post-login

#### APPLICAZIONI D'USO IN LOGOTIPI

Il pittogramma di SPID può essere utilizzato anche come elemento per caratterizzare l'offerta di uno dei diversi Identity-Service Provider, creando una sub-brand. Sotto, alcuni esempi fittizi. Fra logo dell'Identity Provider e pittogramma ci sono sempre almeno 16px di distanza.



IdP immaginari

Le raccomandazioni relative all'applicazione d'uso nei logotipi non riguardano i brand già creati e registrati al 01.06.2018.

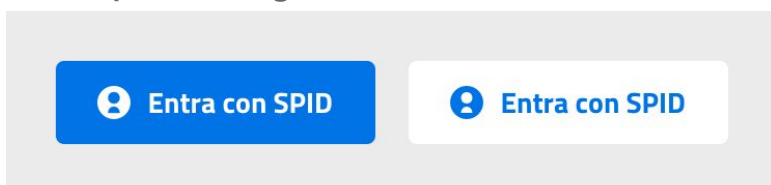
### 2.1.3 Pulsante "Entra con SPID"



In questo specifico pulsante il minimo elemento di brand è sempre accompagnato dal testo della Call-To-Action (azione imperativa del pulsante) a destra, il cui **complemento di mezzo o strumento è 'con SPID', sempre presente in maiuscolo**.

La CTA ad oggi più utilizzata è "Entra", ma non si escludono future declinazioni come "Firma" o "Autorizza", giusto per citarne degli esempi. Questo bottone è lo standard utilizzabile sia per desktop che per mobile, fino ad un massimo di 400px di larghezza.

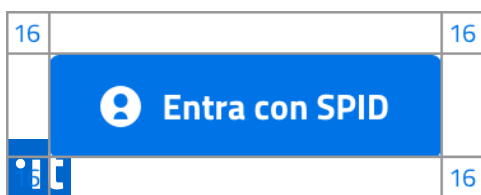
#### Versioni positiva e negativa



Può essere utilizzato:

- Su **sfondo blu** (in positivo) con testi e icona in bianco, se il colore di background è un colore chiaro, con un contrasto inferiore a 3,50:1.
- Su **sfondo bianco** (in negativo) con testi e icona in blu, se il colore di background è invece un colore scuro che supera il contrasto 3,50:1.

#### Area di rispetto



Tutti i bottoni descritti hanno un margine esterno di 16px per ogni lato, costituendo così l'area di rispetto circostante.

### Codici colori e stati



- Il blu #0073E6 corrisponde allo stato di **default**;
- Il blu #0059B3 rappresenta lo stato di **active** – hover in web o pressed in mobile.

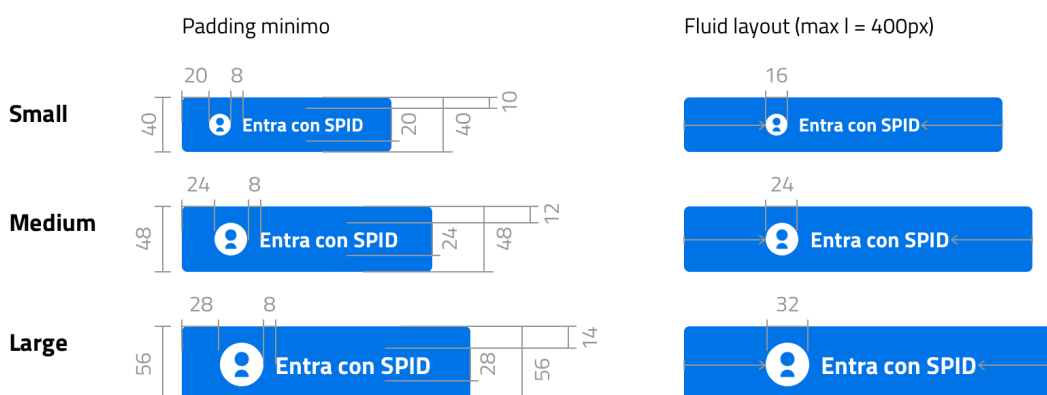
Non sono ammessi ulteriori colori.

### Size, ingombri minimi e padding

Questo pulsante ha tre altezze definite, da cui dipendono specifici padding e relativi font-size. Questo bottone deve **sempre apparire intero** a prescindere dalla tipologia di device: non sono ammesse minimizzazioni cross breakpoint.

Se il bottone aumenta la propria larghezza in base al testo della CTA, vanno seguite le seguenti indicazioni:

- **Small** – altezza di 40px, con padding laterale di 20px. L'icona è grande 16px, mentre il font style utilizzato è Titillium Web Bold, 14px.
- **Medium** – altezza di 48px, con padding laterale di 24px. L'icona è grande 24px, mentre il font style utilizzato è Titillium Web Bold, 16px.
- **Large** – altezza di 56px, con padding laterale di 28px. L'icona è grande 32px, mentre il font style utilizzato è Titillium Web Bold, 18px.

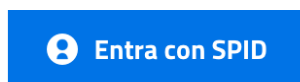


Se invece il bottone è all'interno di un layout fluido, l'icona e il testo della CTA sono sempre centrati in larghezza – **la larghezza massima del bottone non può superare 400px**.  
Fra icona e testo della CTA ci sono sempre 8px di spaziatura.

## Angoli arrotondati e netti



Angoli arrotondati (4px)

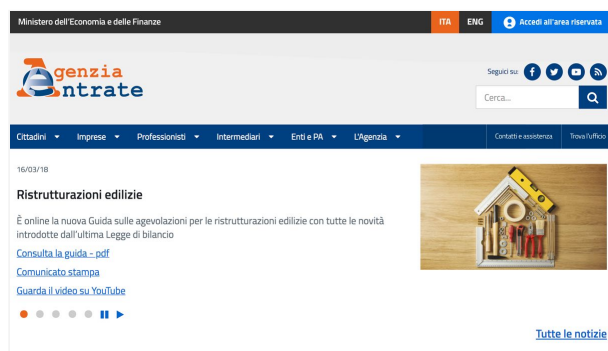


Angoli netti

Il bottone può avere:

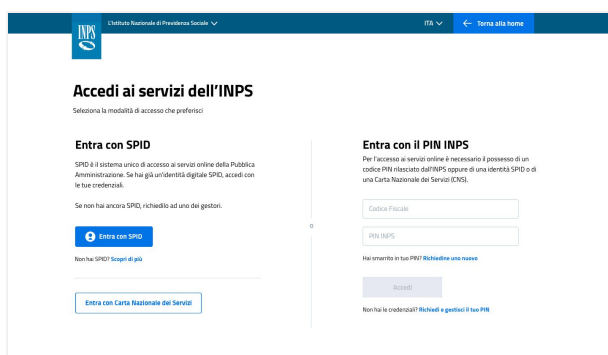
- **Angoli arrotondati**, che rappresentano il bottone standard all'interno del design language di SPID. Nello specifico, l'arrotondamento è sempre di 4px.
- **Angoli netti** solo se il layout e il suo relativo spazio non consente di mettere il pulsante con un'area di rispetto (margine esterno) adeguata alla sua misura.

## Applicazioni d'uso in pagina



ANGOLI NETTI – IN HEADER

In questo esempio, nel sito dell'Agenzia delle Entrate, il bottone ha angoli netti, in quanto inserito nella top header.



ANGOLI ARROTONDATI – IN PAGINA

Nella pagina di disambiguazione del sito dell'INPS, per esempio, il bottone è inserito nel suo formato standard, con angoli arrotondati.

## Raccomandazioni esecutive

I bottoni possono scaricati in SVG dal repository di progetto, ma è preferibile che siano



sviluppati tramite HTML e CSS, per gestire direttamente in codice i diversi elementi (stati del bottone, testo delle CTA, larghezza fluida o fissa – si ricorda che le altezze, invece, sono fisse). Il pittogramma dell'utente – minimo elemento di brand dev'essere incluso nei bottoni come SVG, per non avere problemi di risoluzione.

Tutte le misure sono state definite in px. Nel caso si utilizzassero PNG o si stesse lavorando per monitor retina, si ricorda di moltiplicare le misure per 2 (2x).

## 2.2 Tone of Voice e Lingua

© Questo paragrafo ha carattere di raccomandazione.

*Gli attori del circuito SPID sono invitati a considerare quanto riportato come best-practice e a metterlo in pratica nel progettare le proprie interfacce relative a SPID.*

Il testo usato nelle interfacce dei prodotti digitali gioca un ruolo fondamentale nell'esperienza dell'utente: il testo comunica, informa e guida.

Di seguito sono riportate le regole generali per una comunicazione efficace:

1. Non c'è bisogno di tante parole.

Per progettare una buona user experience, si deve andare dritti al punto di ciò che si vuole comunicare (cosa, come, qual è il valore, ecc.). Evitare di scrivere cose ovvie che l'utente potrebbe già conoscere ed evitare di aggiungere troppi dettagli se questi possono distrarre dal fine ultimo della pagina o della schermata in questione.

2. È importante scegliere cosa dire e quando dirlo.

Posizionate il testo giusto nel momento giusto dell'esperienza: a seconda del momento in cui l'informazione viene data, questa può apparire più o meno utile. La raccomandazione è di dare informazioni generali nelle pagine di presentazione del servizio e informazioni più specifiche, per esempio relative agli strumenti e ai processi, nelle pagine dei processi stessi. In generale va evitata la disomogeneità tra pagine piene di testo e pagine in cui l'utente non sa cosa deve fare.

3. Il testo deve informare e guidare nell'azione.


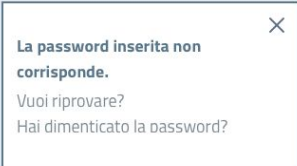

Ogni testo presente nell'interfaccia deve condurre l'utente al passaggio successivo, che sia quello di registrarsi, effettuare il riconoscimento o cercare più informazioni. Vanno evitati i vicoli ciechi nell'esperienza, inserendo sempre call to action anche nelle pagine più "statiche" come ad esempio le pagine di visualizzazione delle Condizioni di Servizio o della Privacy.

Dire la cosa giusta al momento giusto non riguarda solo il COSA e il QUANDO, ma anche il COME viene detto.

SPID è un servizio nazionale che si rivolge a milioni di utenti ciascuno con diverse caratteristiche e necessità. Per questo motivo il tono della comunicazione deve essere ufficiale e allo stesso tempo chiaro, semplice e che infonde sicurezza. Per riuscire a trovare questo equilibrio, il modo migliore è quello di:


1. Identificare un set minimo di informazioni che si vogliono dare nella pagina, siano esse le caratteristiche principali del servizio o le istruzioni per registrarsi al servizio;
2. Spiegare tali contenuti con un linguaggio non tecnico, né burocratico o complicato che sia comprensibile per la ragazza di 18 anni, così come per il pensionato di 80.
3. Testare il copy della pagina con alcuni campioni di utenti per verificarne l'efficacia, anche a livello "emozionale".

Esempi di tone of voice applicato ai messaggi di errore:

		
Ufficiale ✓ Chiaro ✗ Semplice ✓ Che dà sicurezza ✗	Ufficiale ✓ Chiaro ✓ Semplice ✓ Che dà sicurezza ✓	Ufficiale ✗ Chiaro ✓ Semplice ✓ Che dà sicurezza ✗

All'interno del servizio, il linguaggio può assumere toni diversi a seconda del contenuto e della situazione in cui questo viene presentato. Scegliere quello migliore significa tenere sempre a mente cosa si vuole comunicare, a chi si sta parlando in quel momento e il contesto in cui la comunicazione avviene.

## 2.3 Lingue ufficiali

 Questo paragrafo ha carattere normativo.

La lingua ufficiale di SPID è l'italiano. Tuttavia in Italia sono riconosciute e tutelate dalla stessa Costituzione (art. 6) le minoranze linguistiche, in particolare il tedesco e il francese. A tale scopo si richiede agli Identity Provider di fornire l'interfaccia di autenticazione anche in lingua tedesca e francese, e, auspicabilmente, in inglese, per facilitare la diffusione di SPID tra i cittadini italiani residenti all'estero.

Si prevede, quindi, di dare la possibilità di cambiare la lingua all'interno dell'interfaccia, con un selettore multi-lingua posizionato in alto a destra nell'header come da immagine. . Se possibile, su mobile, impostare la lingua prendendo l'informazione dal device.

F.1 - Applicazione del selettore lingua nell'header delle interfacce di accesso con SPID.

## 2.4 Terminologia di SPID

© Questo paragrafo ha carattere di raccomandazione.

Questa sezione raggruppa alcuni dei termini ufficiali da utilizzare relativamente al servizio SPID.

**Identità Digitale:** SPID è un'identità digitale, ovvero una chiave di accesso per accedere ai servizi digitali dei Service Provider accreditati.

**Identity Provider:** Si tratta di quegli enti accreditati, noti come Gestori dell'Identità digitale, che hanno mandato di rilasciare le identità digitali. Questi attori devono attenersi alle linee guida presenti in questo documento nella progettazione delle loro interfacce. In italiano si usa Provider anche quando si usa al plurale.

**Service Provider:** Sono gli enti e le compagnie sia pubblici che privati, noti come Fornitori di Servizi, che permettono ai propri utenti di accedere ai loro servizi tramite SPID. Questi attori devono attenersi alle linee guida presenti in questo documento nella progettazione delle loro interfacce. In italiano si usa Provider anche quando si usa al plurale.

**Credenziali:** Si usa per riferirsi alla coppia nome utente e password.  
*Es. Accedi al servizio utilizzando le tue credenziali SPID.*

**Nome utente:** Deve essere usato per riferirsi all'indirizzo e-mail, al codice fiscale o alla stringa testuale utilizzati come nome utente di SPID. All'interno delle maschere di accesso non deve essere usata la versione in inglese "username". Quando il nome utente è l'indirizzo e-mail o il C.F., può essere esplicitato direttamente.

# 03 User Experience, Template e Flussi

## 3.1 Introduzione

❖ Questo paragrafo ha carattere informativo.

In questa sezione verranno descritti i flussi e il layout delle interfacce principali per l'integrazione di SPID, sia dal lato degli Identity Provider ([Capitolo 3.2](#)), sia dal lato dei Service Provider ([Capitolo 3.3](#)).

I flussi e template qui descritti, possono essere illustrati in forma di wireframe o di interfaccia grafica definitiva. Il wireframe è una rappresentazione astratta che ha lo scopo di definire la struttura della pagina e il comportamento dei vari elementi dal punto di vista funzionale, pertanto non deve essere inteso come riferimento per la grafica definitiva della pagina. Quando l'immagine è descritta come interfaccia grafica definitiva, si richiede all'Identity o Service Provider di implementare il flusso o il template in oggetto esattamente come definito nell'immagine.

Le didascalie delle immagini specificano la tipologia di rappresentazione mediante le etichette: [wireframe] o [grafica].

I flussi e i template definiti nei prossimi capitoli sono stati sviluppati secondo le linee guida di design create e diffuse dal Team per la Trasformazione Digitale e AgID e devono essere implementati in modo corretto.

## 3.2 Flussi e Template per gli Identity Provider

### 3.2.1 Pagina Informativa

👉 Questo paragrafo ha carattere normativo.

Ogni Identity Provider deve avere una pagina informativa che descrive il servizio SPID. La pagina si rivolge principalmente agli utenti che non conoscono o ancora non hanno un'identità SPID. Per questo motivo i contenuti vanno realizzati attorno a 4 temi:

- Cos'è SPID?
- Come si usa?
- Cosa mi permette di fare?
- Come posso ottenerlo?

Nel definire "cos'è SPID" deve essere specificato che i servizi offerti dall'Identity Provider sono strumenti che consentono di accedere ai servizi online di Pubbliche Amministrazioni e

privati che sono parte del circuito SPID. Devono inoltre essere chiaramente indicati i tre livelli di sicurezza e le differenti caratteristiche di ciascuno.

Nella parte relativa a cosa mi permette di fare, non è necessario visualizzare una lista esaustiva di tutti i servizi, ma è sufficiente dare delle indicazioni di alto livello e fornire il link al sito <https://www.spid.gov.it/servizi>, che costituisce l'archivio di tutti i servizi a cui si può accedere con SPID.


Nelle indicazioni su "come ottenere l'identità digitale" devono essere chiaramente indicate:

- le modalità di riconoscimento dell'utente utilizzate dal gestore per il rilascio dell'identità digitale SPID, informando in maniera puntuale sulla strumentazione necessaria per ciascuna modalità;
- le tempistiche medie di ottenimento con la modalità scelta (anche caricando automaticamente le statistiche SPID di ogni Identity Provider);
- eventuali costi accessori (evidenziando che non si tratta del pagamento dell'identità, ma di una facilitazione commerciale a supporto del suo ottenimento).

Per maggiori informazioni sui contenuti, vedere il capitolo [01 Il sistema SPID](#).

Nella pagina deve essere presente e visibile sin da subito il logo SPID (per le regole di utilizzo degli asset grafici di SPID, vedere il [capitolo 2.1](#)) unitamente alla call to action per avviare il flusso di registrazione. Inoltre, la pagina del sito deve rimandare al sito istituzionale [www.spid.gov.it](http://www.spid.gov.it).

### 3.2.2 Flusso di Registrazione

 Questo contenuto ha carattere normativo.

Il flusso di ottenimento di SPID è il primo momento della reale interazione del cittadino con il sistema dell'identità digitale, nonché il passaggio cruciale della sua adozione. Gli Identity Provider sono quindi tenuti a semplificare il più possibile il flusso di registrazione, guidando l'utente in maniera chiara e riducendo il numero di passaggi necessari all'ottenimento di SPID, che devono attestarsi nell'ordine dei 5-10.

 Questo contenuto ha carattere di raccomandazione.

Di seguito viene illustrato il flusso di registrazione di riferimento.

Il processo di registrazione si compone di 5 step principali:

1. Selezione del tipo di SPID richiesto e del metodo di riconoscimento
2. Log-in con un eventuale account già esistente / Inserimento dati anagrafici, documenti e di contatto
3. Visualizzazione delle condizioni generali di servizio e della privacy
4. Scelta delle credenziali per l'account SPID
5. Riconoscimento

Nel caso in cui il metodo di riconoscimento selezionato sia a pagamento, gli step saranno 6 e potrebbero comportarsi in questo modo:

1. Selezione del tipo di SPID richiesto e del metodo di riconoscimento

2. Log-in con un eventuale account già esistente / Inserimento dati anagrafici e di contatto
3. Visualizzazione delle condizioni generali di servizio e della privacy
4. Scelta delle credenziali per l'account SPID
5. Pagamento
6. Riconoscimento.

A seconda di necessità specifiche e/o di rispetto di eventuali policy aziendali, gli Identity Provider potrebbe voler riordinare i diversi passaggi diversamente (es. 1, 2, 4, 3, 5, 6 oppure 1, 4, 3, 2, 5, 6).


Si richiede agli Identity Provider che richiedono il pagamento prima del rilascio dell'identità, di coprire il caso in cui a pagamento avvenuto, dovessero verificarsi problemi nel rilascio l'identità, garantendo l'eventuale rimborso del cittadino.

Le pagine del flusso di registrazione devono sempre mostrare il logo di SPID, unitamente al logo dell'identità dell'Identity Provider, e uno stepper che permetta all'utente di orientarsi nei diversi passaggi del processo.



F.2 - Esempio di header, titolo di pagina e stepper relativi al flusso di registrazione [wireframe]

### 3.2.2.1 Selezione del tipo di SPID richiesto e del metodo di riconoscimento


 Questo paragrafo ha carattere normativo.

In questo passaggio si domanda al cittadino:

- se vuole richiedere un'identità SPID per uso personale o professionale;
- in che modo vuole essere riconosciuto, esplicitando eventuali costi relativi alle modalità di riconoscimento disponibili\*.

\*N.B. Va comunicato espressamente a che titolo è previsto il pagamento, ove previsto.

### 3.2.2.2 Log-in con un eventuale account già esistente / Inserimento dati anagrafici e di contatto

 Questo paragrafo ha carattere normativo.

Il passaggio richiede l'inserimento dei seguenti dati:

1. Dati anagrafici;
2. Domicilio;

3. Dati di contatto;
4. Estremi del documento di identità.

Per le persone fisiche sono obbligatorie le seguenti informazioni:


- nome e cognome
- codice fiscale (C.F.)
- sesso (derivabile dal C.F.)
- data di nascita (derivabile dal C.F.)
- luogo di nascita
- indirizzo di domicilio
- numero di cellulare - da verificare\*
- indirizzo e-mail - da verificare\*
- numero di tessera sanitaria
- estremi di un valido documento di identità (e relative scansioni se necessarie per il metodo di riconoscimento prescelto)

Quando possibile, prepopolare i dati anagrafici di cui già si dispone, quando l'utente è loggato, oppure richiedendo di effettuare l'accesso.

Qualunque altra informazione richiesta all'interno del flusso di registrazione all'identità SPID deve essere chiaramente caratterizzata come non obbligatoria e deve essere esplicitato il motivo per cui viene richiesta. Si sconsiglia tuttavia di appesantire il processo di registrazione, dal momento che è possibile richiedere dettagli aggiuntivi all'interno della pagina di gestione dell'identità, in maniera non obbligatoria.

\*Per verificare i dati di contatto, l'utente dovrà inserire un codice che gli verrà inviato sul rispettivo canale di contatto. Senza verifica, il processo non può continuare.

### **3.2.2.3 Visualizzazione delle condizioni generali di servizio e della privacy**


 Questo paragrafo ha carattere normativo.

In questa sezione l'utente visualizza e accetta le condizioni generali di servizio e privacy che devono essere attinenti e necessarie al servizio d'identità digitale SPID.

L'accettazione di tali clausole è obbligatoria per poter continuare il processo.

Dovranno essere chiaramente distinte le clausole di accettazione per l'ottenimento dell'identità digitale SPID da quelle, eventuali, di natura commerciale e di marketing.

### **3.2.2.4 Scelta delle credenziali per l'account SPID**

 Questo paragrafo ha carattere normativo.

In questo passaggio, l'utente inserisce il nome utente e la password che utilizzerà per il suo account SPID.

Il nome utente deve essere un'informazione legata al cittadino, quanto più stabile nel tempo e con cui l'utente ha confidenza.


Al momento attuale sono utilizzati l'indirizzo e-mail, (o) il codice fiscale o una stringa testuale (lettere e numeri).

Per l'uso di indirizzi e-mail, si consiglia di specificare, in fase di registrazione, che è meglio siano personali e non professionali, quanto meno per le identità SPID per persona fisica, perché più stabili nel tempo.

I criteri di creazione della password (es. lunghezza minima, caratteri speciali, ecc.) devono essere sempre ben visibili all'utente. Qualora il cittadino scelga una password non conforme ai criteri definiti, è necessario che l'Identity Provider indichi puntualmente quale criterio non è stato rispettato.

Si raccomanda, in fase di creazione della password, di utilizzare un indicatore di sicurezza (password meter), in modo da fornire tale informazione al cittadino.

### 3.2.2.5 Riconoscimento

 Questo paragrafo ha carattere normativo.

In questo passaggio, verranno date all'utente le istruzioni necessarie per effettuare il riconoscimento, nel caso questo sia asincrono. Ad esempio viene fatto un riepilogo di documenti da portare al punto fisico in cui ci si deve recare per fare un riconoscimento *de visu*. Oppure, viene preso appuntamento per richiedere il riconoscimento via webcam, ecc. Qualora la modalità di riconoscimento possa avvenire in maniera sincrona, ovvero contestualmente al processo in corso, attraverso altri strumenti già in possesso dell'utente, si può anticipare questo passaggio, posizionandolo prima dello step 2. Gli strumenti ammissibili devono essere proposti dall'Identity Provider e approvati da AgID caso per caso.



F.3 - Esempio di ordine dei passaggi in cui il riconoscimento avviene in maniera sincrona e quindi prima di scegliere le credenziali [wireframe]

In caso di modalità di riconoscimento a **pagamento**, il flusso di pagamento segue gli standard del sito in cui viene erogato.

Anche in questo caso, deve essere chiaro al cittadino che non sta pagando SPID, ma che sta pagando perché ha richiesto un certo tipo di riconoscimento.





F.4 - Esempio di stepper nel caso in cui si debba effettuare il pagamento prima del riconoscimento [wireframe]

Esiste un ultimo caso, quello del riuso delle identità pregresse, in cui il flusso di registrazione non ha più bisogno dello step di Riconoscimento, perchè il Service Provider garantisce che quell'identità sia propria della persona che la sta usando. Per approfondire si rimanda al paragrafo [3.3.2 Procedure di Registrazione Assistita e Riuso delle Identità Pregresse](#).

### 3.2.3 Flussi di Accesso

 Questo paragrafo ha carattere normativo.

L'utente che vuole usufruire di un servizio utilizzando SPID, deve portare a termine il flusso di accesso relativo al livello di sicurezza che tale servizio richiede. Per un approfondimento sui diversi livelli di sicurezza di SPID, si rimanda al capitolo [1.2 Credenziali e Livelli](#).

Ogni flusso di accesso inizia attraverso un click:

- sullo [smart button](#), che permette di scegliere il proprio Identity Provider quando l'utente non ha ancora aperto una sessione SPID;
- su una call to action che apre direttamente la schermata relativa al flusso di autenticazione richiesta, nel caso l'utente abbia già compiuto l'accesso con nome utente e password di SPID e effettui la nuova richiesta entro la durata della sessione. Per approfondire questo tema, si rimanda al capitolo [1.4 Sessioni, Single Sign On e Passaggi di Livello](#).

Le interfacce per gli Identity Provider sono rilasciate in formato html/css/javascript in modo da essere facilmente implementate nel sistema di autenticazione. Sono già testate dal punto di vista di responsività, accessibilità e risultano conformi alle linee guida di design per i siti della Pubblica Amministrazione. I file sono forniti da AgID e scaricabili dal repository di progetto. Nessuno degli elementi del design (es. font, colori, stili, dimensioni dei loghi) deve essere modificato.

I flussi sono definiti tecnicamente nel documento relativo alle [Regole Tecniche](#).

Da qualunque schermata dei flussi di accesso, l'utente può cliccare Annulla per uscire dal flusso. L'uscita dal flusso atterra sulla pagina di inizio flusso lato del Service Provider.

N.B. Gli Identity Provider sono liberi di far accedere l'utente con un livello più alto rispetto a quanto richiesto dal servizio, se questo comporta un miglioramento dell'esperienza. In tal

caso la pagina di accesso contiene gli elementi necessari a svolgere sia l'autenticazione di livello x, sia l'autenticazione di livello  $y > x$ .

## Primo livello

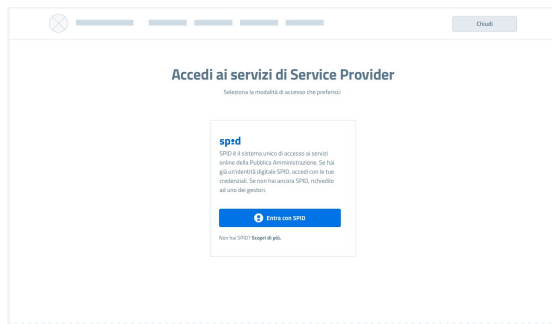
Il flusso di primo livello consiste nell'inserimento di nome utente (e-mail, codice fiscale o stringa) e password.

Nel caso in cui l'utente inserisca delle credenziali non corrette, l'errore verrà visualizzato direttamente in linea. C'è un numero massimo di tentativi per reinserire le credenziali. Una volta esauriti i tentativi, l'account dell'utente viene bloccato e viene visualizzato un errore. Per un approfondimento sui messaggi di errore, si rimanda al capitolo [3.4 Errori e Notifiche di utilizzo](#).

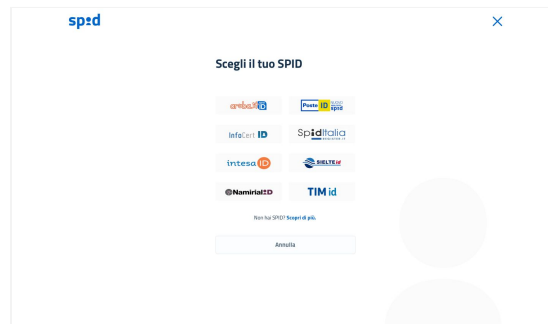
Se il servizio a cui si sta accedendo richiede un livello di sicurezza 1, una volta inserite le credenziali esatte, l'utente visualizza la pagina di autorizzazione al passaggio dei dati che riporta la lista di quali dati stanno per essere comunicati al Service Provider. Dopo la conferma viene rediretto al sito del Service Provider.

Se invece il servizio richiede un livello di sicurezza maggiore, viene visualizzata la prima schermata relativa al flusso di livello successivo.

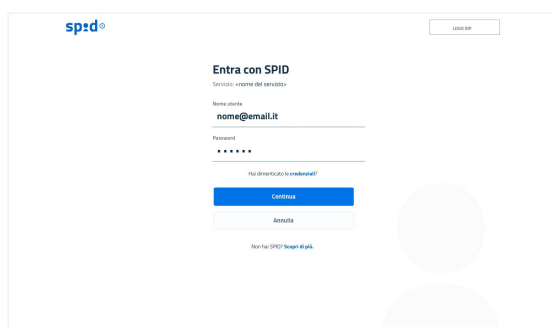
Esempio di flusso di accesso di primo livello su web:



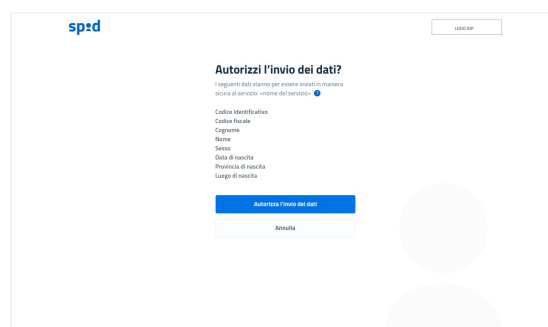
F.5 - Pagina di accesso di un generico Service Provider [wireframe]



F.6 - Pagina di selezione degli Identity Provider [grafica]



F.7 - Pagina di inserimento credenziali [grafica]



F.8 - Pagina di autorizzazione al passaggio dei dati [grafica]

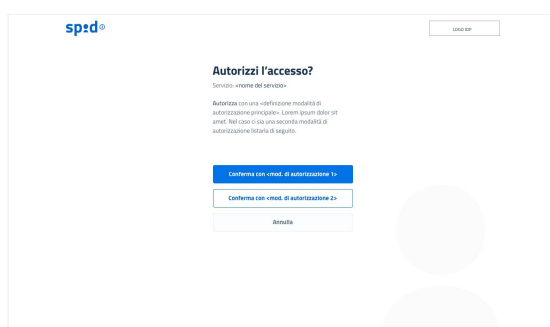
Nel caso in cui l'Identity Provider metta a disposizione ulteriori modalità di accesso (ad esempio tramite app), l'interfaccia può essere adattata di conseguenza.

## Secondo livello;

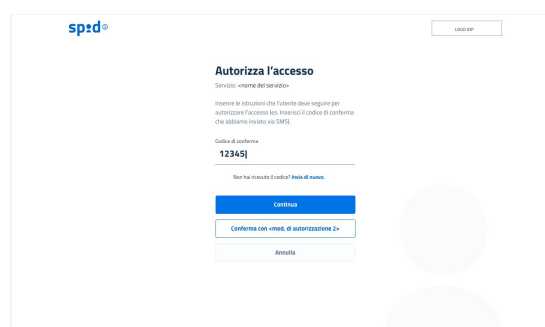
Il flusso di secondo livello consiste nell'inserire un codice di verifica temporaneo che viene spedito via SMS sul numero registrato oppure generato da un'app mobile su un dispositivo certificato. Come specificato nel paragrafo [Livello 2 - Codice temporaneo o Fattore biometrico](#), il codice di verifica temporaneo può essere rafforzato, permettendo all'utente di utilizzare un fattore biometrico, ad esempio l'impronta digitale.

In questo caso è importante notare che per motivi di sicurezza, una volta emesso il codice di verifica, l'utente può inserirlo entro un tempo massimo dalla sua emissione. Se il tempo dovesse scadere senza che l'utente abbia completato il processo, l'interfaccia deve essere modificata, impedendo di inserire un codice già scaduto, ma permettendo all'utente di richiederne uno nuovo o, se disponibile, di scegliere un'altra modalità di autenticazione.

Esempio di flusso di accesso di secondo livello su web:



F.9 - Pagina di selezione della modalità di autorizzazione (es. SMS o app) [grafica]



F.10 - Pagina di inserimento codice di verifica [grafica]

## Terzo livello.

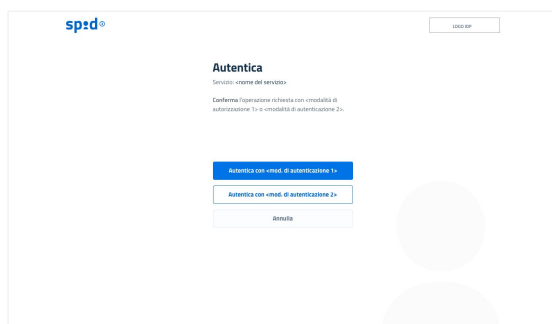
Il flusso di terzo livello consiste nell'utilizzare un device per accedere al servizio.

Mentre il livello 1 e 2 fanno parte del set di credenziali minimo per utilizzare SPID, il livello 3 è un livello che l'utente può o non può richiedere in fase di registrazione a SPID. Di conseguenza in un flusso che richiede un'autenticazione di terzo livello possono verificarsi i seguenti casi:

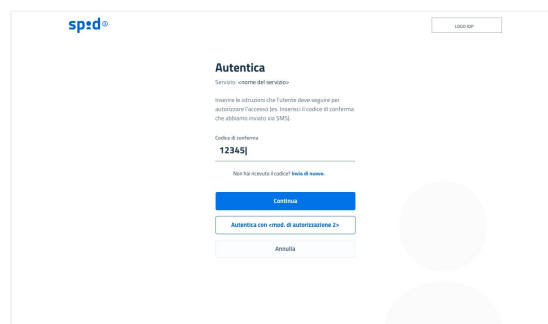
1. l'utente è in possesso dello strumento per effettuare un accesso di livello 3. In questo caso, l'utente viene rediretto al normale flusso di autenticazione previsto dall'Identity Provider.

2. l'utente non è in possesso dello strumento per effettuare un accesso di livello 3, anche se il suo Identity Provider lo fornisce. In questo caso, l'Identity Provider mostra all'utente viene mostrata una schermata di errore con le informazioni relative alla possibilità di ottenere lo strumento per permettere il livello 3.
3. l'utente non è in possesso dello strumento per effettuare un accesso di livello 3, perchè l'Identity Provider con cui è loggato, non lo eroga. In questo caso, il Service Provider riconduce alla pagina di selezione dell'Identity Provider con l'informazione relativa all'impossibilità di accedere al servizio con quella identità SPID.

Esempio di flusso di accesso di terzo livello su web:




F.11 - Pagina di selezione dello strumento di autenticazione [grafica]



F.12 - Pagina di inserimento codice di verifica [grafica]

### 3.2.4 Pagina di Gestione dell'Identità SPID

 Questo paragrafo ha carattere normativo.

La gestione dell'identità SPID e in particolare dell'aggiornamento dei dati anagrafici dell'utente, avviene in un'apposita area del sito dell'Identity Provider, così come descritto nell'articolo 19 del [Regolamento delle Modalità Attuative](#).

Non deve essere confusa con l'area post-login dei diversi Service Provider o degli account proprietari - non abilitati a SPID - degli Identity Provider stessi.

Le funzionalità e le informazioni presenti in quest'area devono essere compliant con il nuovo Regolamento Europeo in materia di Privacy (GDPR).

Dall'area di gestione della propria identità SPID, l'utente potrà sempre visualizzare:

- i dati relativi alla propria identità SPID (codice identificativo, credenziali, livelli, ecc);
- i propri dati anagrafici associati a SPID;
- visualizzazione e gestione dei consensi sulla privacy;
- visualizzazione e download del contratto;
- la lista degli accessi effettuati (se disponibile).

Le funzionalità disponibili per l'utente in quest'area sono:

- richiesta nuove credenziali;
- modifica della password;

- revoca definitiva del profilo con conseguente disattivazione delle credenziali e cancellazione dei dati dell'utente;
- processi di sospensione/riattivazione del servizio;
- gestione delle preferenze sulle notifiche;
- upgrade a livello 3 (se disponibile);
- cambio strumenti per livello 3: comunicazione issue + richiesta e attivazione nuovo strumento (se disponibile);
- richiesta di uno SPID per soggetto rappresentato (se disponibile).

### **3.3 Flussi per i Service Provider**

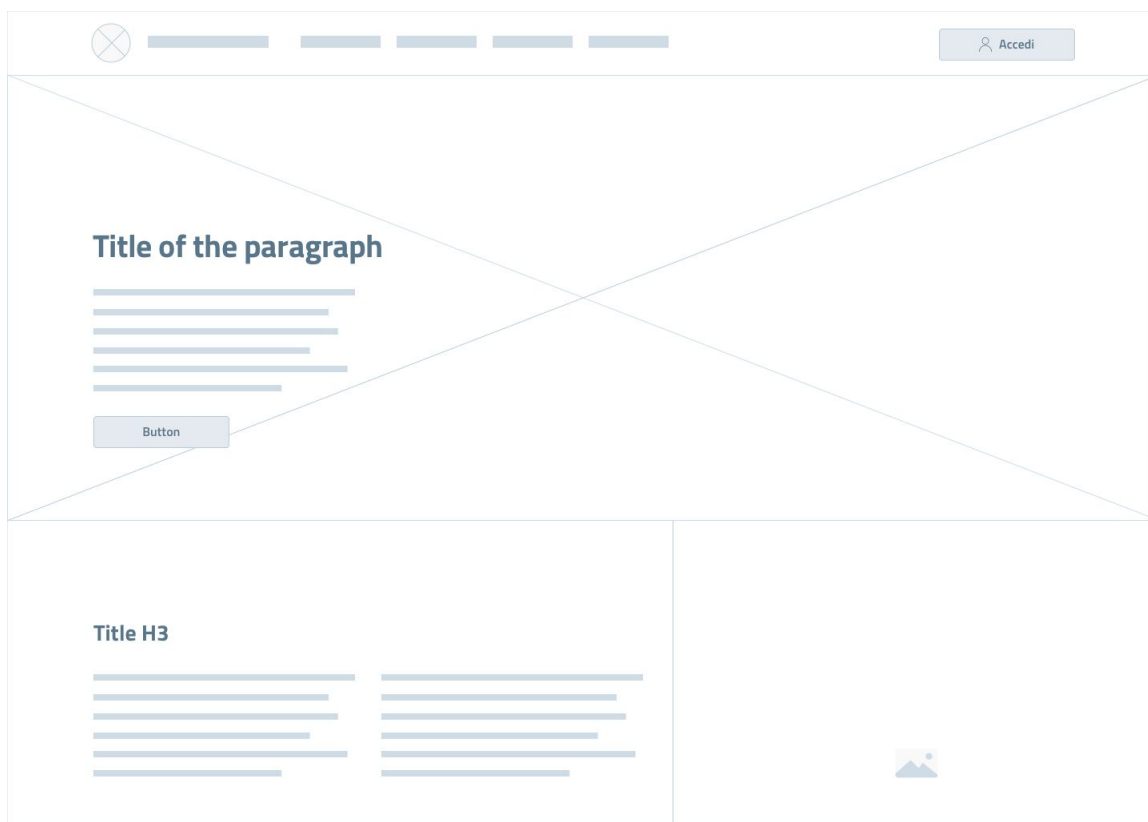
I Service Provider convenzionati permetteranno a tutti i cittadini di accedere ai propri servizi con la loro identità digitale SPID. In questo senso, dovranno integrare l'accesso con tutte le identità SPID di tutte gli Identity Provider, senza eccezioni. Nel caso in cui problemi tecnici o di sicurezza impediscano l'integrazione di un certo tipo di identità, si prega di segnalarlo all'helpdesk di AgID.

#### **3.3.1 Pulsante di Accesso**

 Questo paragrafo ha carattere normativo per i Service Provider pubblici.

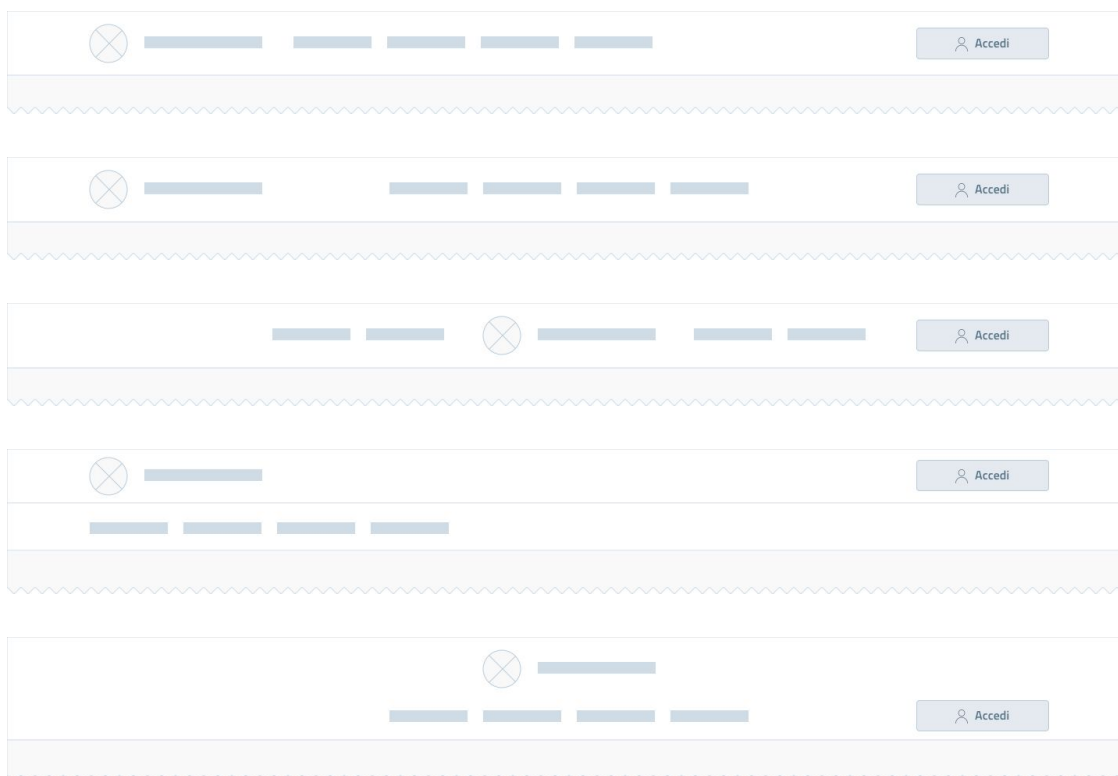
##### **3.3.1.1 Posizionamento del pulsante di accesso**

Il pulsante di login per accedere ai servizi o all'area personale va sempre posizionato in alto a destra nella pagina. La best practice chiede di inserirlo all'interno dell'header in modo che sia sempre facilmente individuabile dall'utente, in una posizione costante per tutte le pagine del sito.



F.13 - Esempio di posizionamento del pulsante di accesso all'area riservata sul sito di un generico Service Provider [wireframe]

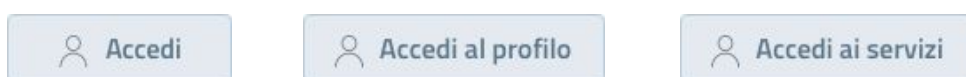
Di seguito riportiamo alcuni esempi di come posizionare il pulsante a seconda della struttura grafica dell'header:



### 3.3.1.2 Label del pulsante di accesso

È buona norma che i pulsanti descrivano l'azione che permettono all'utente di svolgere. Per questo motivo consigliamo di utilizzare dei verbi come etichetta dei pulsanti, possibilmente in tutto il sito.

Sia che il servizio preveda l'accesso solo con SPID (SPID only), sia che siano previste più modalità di accesso, la label del pulsante dev'essere *Accedi*, oppure *Accedi ai servizi*, oppure ancora *Accedi all'area personale*, a seconda dello spazio disponibile e del tipo di attività disponibili nell'area post-login del sito in questione.



F.15 Esempi di pulsanti di accesso. La struttura è sempre Icona + Label [wireframe]

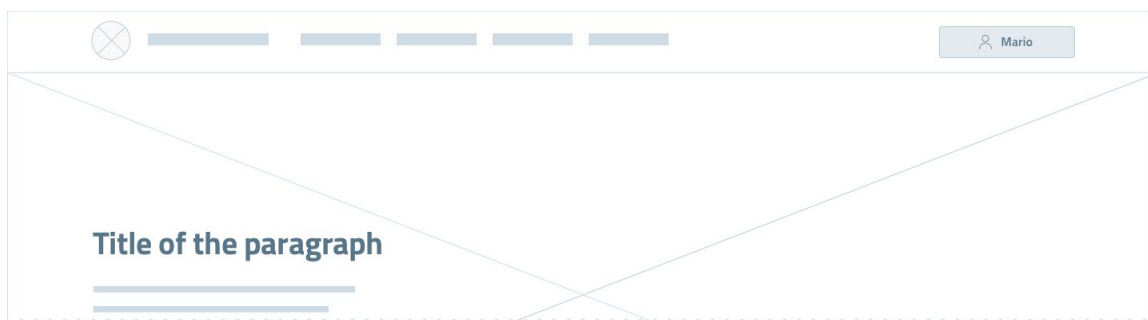
Se il sito prevede una versione in inglese, la label diventerà *Log-in*.

Lo stile del bottone segue i fogli di stile del sito del Service Provider. Tuttavia, se prevede anche l'utilizzo di SPID, deve includere l'icona utente scaricabile dai repository di progetto. Non si danno specifiche a livello di spaziature e allineamenti degli elementi all'interno del bottone, perché queste seguiranno i Css del sito.

Al click dell'utente sul pulsante *Accedi*, il sito richiama la pagina di disambiguazione in cui l'utente riceve informazioni circa la o le modalità di accesso.

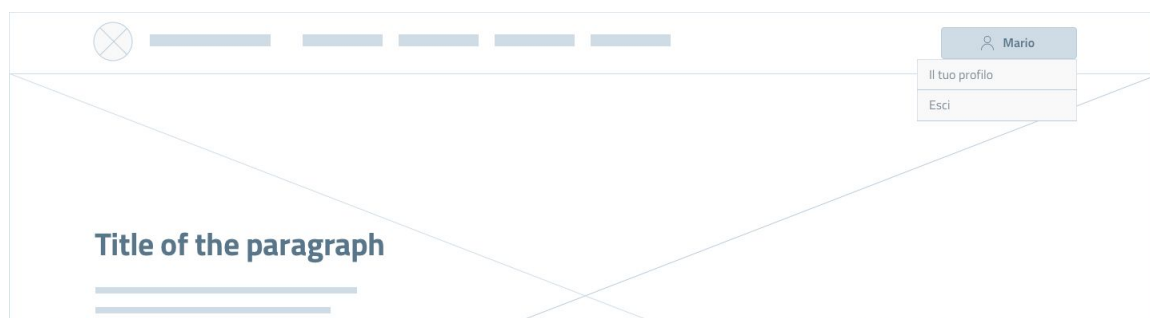
### 3.3.1.3 Utente già loggato

Quando l'utente accede al servizio, il pulsante *Accedi* in alto a destra dell'header, esporrà il nome del cittadino. Qualora il Service Provider non abbia ricevuto tra le informazioni il nome utente, può usare un generico "Utente autenticato" o soluzioni che risolvano l'anonimità (come ad esempio i nomi di animali di Google Drive).



F.21 - Esempio di trasformazione del pulsante di Accesso con utente loggato [wireframe]

Lo stesso pulsante deve fornire all'utente almeno la possibilità di accedere alla propria area personale presso il Service Provider, se presente, e di uscire del servizio, tramite menu a tendina o re-direzionando l'utente a una pagina da cui può visualizzare i suoi dati e uscire dal servizio.



F.22 - Esempio di dropdown che permette all'utente di visualizzare il proprio profilo e/o di uscire dal servizio [wireframe]

Quando l'utente effettua il logout dal servizio, sta effettivamente uscendo del servizio e terminando la sessione di SPID presso l'Identity Provider.

### 3.3.2 Pagina di Disambiguazione

☞ Questo paragrafo ha carattere normativo per i Service Provider pubblici.

La pagina di disambiguazione permette all'utente di visualizzare e selezionare la modalità di accesso che preferisce tra quelle disponibili.

Si possono verificare i seguenti scenari che impattano sulla struttura della pagina:

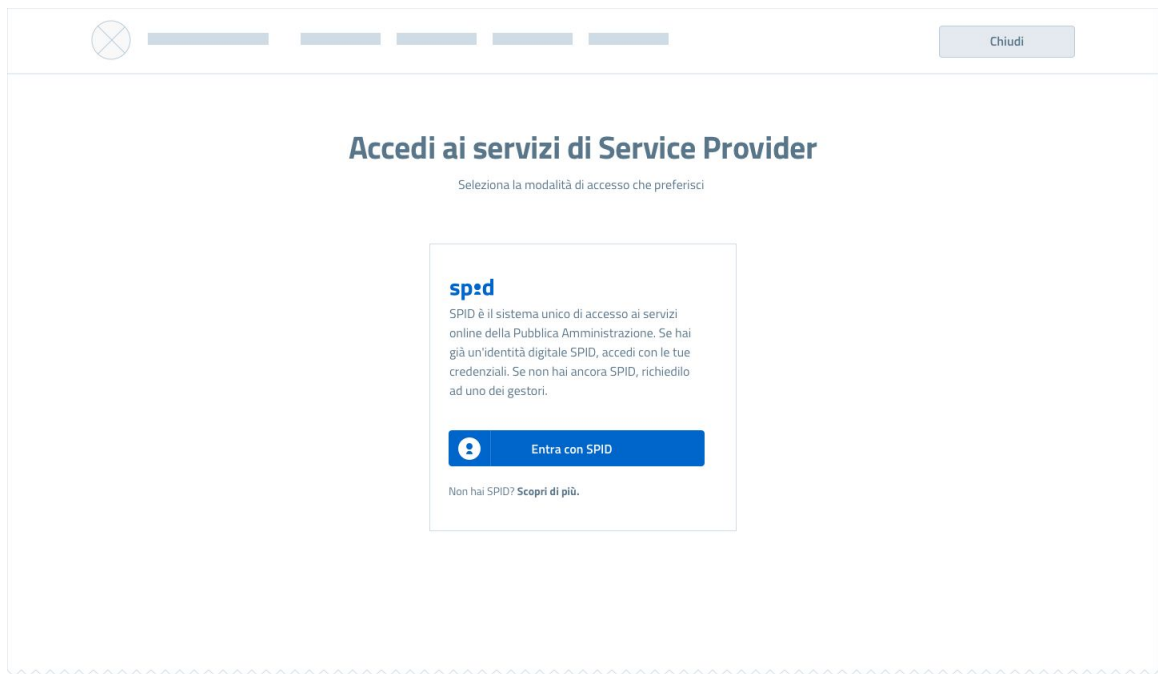
1. I servizi sono accessibili con SPID o CNS. Nel caso di Service Provider privati a queste modalità di accesso si aggiungono eventuali social login.
2. I servizi sono accessibili con SPID (e/o le altre modalità descritte al punto 1) più un'altra modalità che prevede l'inserimento di credenziali (es. nome utente e password, pin, ecc.).
3. I servizi sono accessibili con SPID (e/o le altre modalità descritte al punto 1) più almeno altre due modalità che prevedono l'inserimento di credenziali (es. nome utente e password, pin, ecc.).
4. In tutti gli scenari citati, dal 29 settembre 2018, si aggiungerà anche la possibilità di accedere al servizio tramite eIDAS, che prevede il riconoscimento obbligatorio transfrontaliero dei sistemi di identificazione elettronica notificati dagli Stati membri dell'Unione Europea.

#### Scenario 1

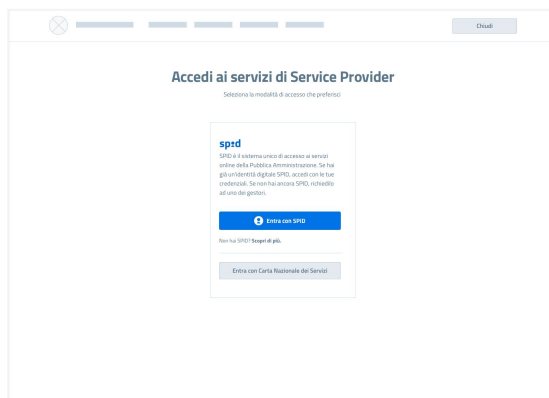
In questo caso, la pagina mostrerà come prima opzione il pulsante *Entra con SPID*, il link *Non hai SPID. Scopri di più.* e, successivamente, i pulsanti relativi alle altre modalità di accesso, in un'unica colonna, in quest'ordine:

- SPID
- CNS
- Eventuali social login (es. Facebook, Google, ecc.).

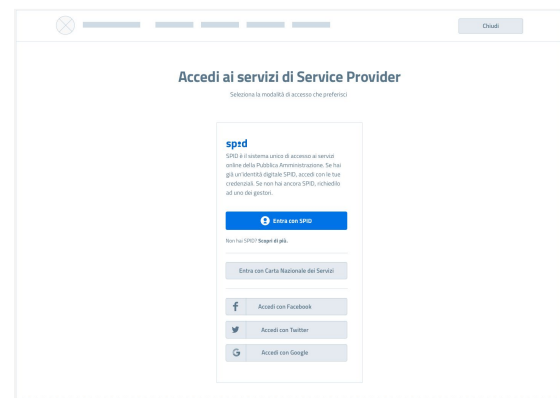




F.16 - Esempio di pagina di disambiguazione in un servizio SPID-only [wireframe]



F.17 - Servizio accessibile con SPID e CNS [wireframe]



F.18 - Servizio accessibile con SPID, CNS e social login [wireframe]

## Scenario 2

In questo caso, la pagina presenterà come prima scelta le modalità citate al punto 1 e, successivamente, il form di login relativo alla seconda modalità di accesso disponibile, con le relative opzioni.


Chiudi

## Accedi ai servizi di Service Provider

Seleziona la modalità di accesso che preferisci

**spid**

SPID è il sistema unico di accesso ai servizi online della Pubblica Amministrazione. Se hai già un'identità digitale SPID, accedi con le tue credenziali. Se non hai ancora SPID, richiedilo ad uno dei gestori.

 **Entra con SPID**

Non hai SPID? [Scopri di più.](#)

**Entra con le tue credenziali**

Lorem ipsum dolor sit amet

Nome utente

Password

Hai dimenticato la password? [Richiedine una nuova.](#)

**Accedi**

Non hai un account? [Registrati.](#)

F.19 - Esempio di servizio accessibile con SPID e con una modalità classica username/password

### Scenario 3

In questo caso, la pagina presenterà come prima scelta le modalità citate al punto 1. In seconda posizione verrà mostrato un modulo contenente tante tab quante sono le modalità di accesso specifiche, ordinate in base alla diffusione delle relative credenziali tra gli utenti.

F.20 - Esempio di servizio accessibile con SPID e con più di una modalità classica nome utente/password [wireframe]

Nel caso di Service Provider privati, l'ordine di presentazione delle opzioni di accesso può essere rivisto.

### 3.3.2.2 Utente non registrato

 Questo paragrafo ha carattere normativo per i Service Provider pubblici.


Per l'utente che non è ancora registrato, non esisterà un pulsante di registrazione al servizio nell'header. Al fine di spingere l'adozione di SPID, mostreremo il link *Non hai SPID? Scopri di più.* direttamente sotto al bottone nella pagina di disambiguazione, come in figura F.16. Al click sul link, l'utente sarà rediretto al sito [spid.gov.it](https://spid.gov.it), il quale si aprirà in una nuova tab del browser.

Per quanto riguarda le altre modalità di accesso:

- CNS e i social login non hanno un corrispettivo del link *Non hai SPID? Scopri di più.*
- Le modalità di registrazioni "tradizionali" (es. username e password, pin, ecc.) mostreranno sotto al form di inserimento delle credenziali il link *Non hai un account? Registrati.*, come in figura F.19.

Qualora non sia necessario per specifiche caratteristiche del servizio, dimostrabili pubblicamente, si raccomanda ai Service Provider pubblici, di non creare ulteriori credenziali che non siano SPID.

### 3.3.3 Il Pulsante *Entra con SPID*

 Questo paragrafo ha carattere normativo.

Il pulsante *Entra con SPID*, anche noto come Smart Button, è l'unico possibile entry point del flusso di accesso con SPID.



F.21 - Il pulsante Entra con SPID, o Smart Button [grafica]

Il pulsante, riprodotto nella figura F.21, non deve essere personalizzato a piacere, ma mantiene la forma e il comportamento in qualunque caso venga integrato.

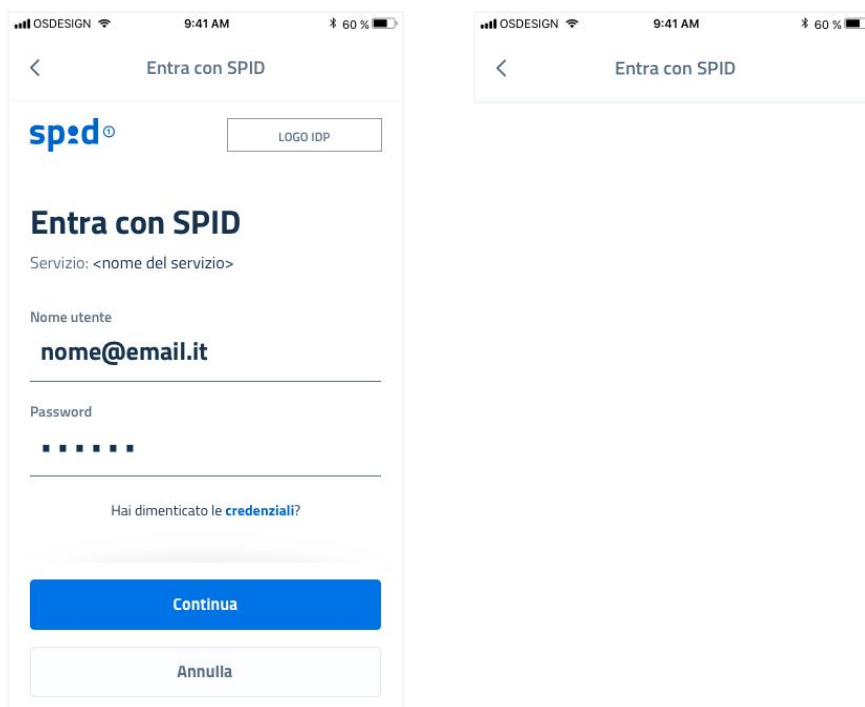
Al click sul pulsante, il sito del Service Provider richiama il primo step di login con SPID, ovvero la pagina di selezione dell'Identity Provider, in cui i loghi delle identità degli Identity Provider sono mostrati in ordine alfabetico.

Lo Smart Button è fornito da AgID e disponibile nel repository di progetto. Si raccomanda di integrarlo richiamando dinamicamente la versione, costantemente aggiornata, resa disponibile via Content Delivery Network.

#### 3.3.3.1 Applicazioni mobili e webview

 Questo paragrafo ha carattere normativo per i Service Provider pubblici.


All'interno delle applicazioni mobile, è possibile integrare il pulsante Entra con SPID. Tuttavia il flusso di accesso sarà visualizzato all'interno di una webview che richiamerà la versione mobile del flusso di login. Si raccomanda di proteggere la webview con i meccanismi più sicuri messi a disposizione dai sistemi operativi al fine di ottenere il massimo isolamento dall'applicazione chiamante.



F.22 - Esempio di topbar della webview per richiamare i flussi di accesso con SPID da applicazioni mobile [wireframe]

La webview in questione deve prevedere solo una top bar e non una bottom bar. Nella top bar dev'essere presente il pulsante Back che permette all'utente di tornare allo step precedente (di chiudere la webview se si trova alla pagina di selezione degli Identity Provider) e l'indicazione Entra con SPID come titolo. Per terminare il flusso, e quindi chiudere la Webview, l'utente potrà anche utilizzare il pulsante Annulla, interno al contenuto della pagina web.

### 3.3.3.2 Caso di Identity Provider che usa il proprio SPID (in maniera esclusiva rispetto agli SPID di altri Identity Provider) per far accedere ai propri servizi.


 Questo paragrafo ha carattere normativo.

In questo caso l'Identity Provider è libero di esporre il logo del proprio servizio di autenticazione, ma senza utilizzare il logo di SPID o fare riferimento a SPID nel testo che lo accompagna.

L'Identity Provider in questione dovrà utilizzare un'implementazione distinta da quella di SPID, in questo sistema di autenticazione parallelo.

Questa misura serve a comunicare chiaramente i requisiti di accesso al servizio agli utenti e ad evitare l'imputazione di eventuali malfunzionamenti a SPID.

### 3.3.3.3 Quando il Service Provider ha bisogno di dati aggiuntivi

 Questo paragrafo ha carattere normativo.

L'utilizzo di SPID è garanzia di sicurezza e semplicità per i cittadini e permette ai Service Provider di accedere ai dati degli utenti, senza sviluppare processi di registrazione o form di inserimento di dati anagrafici complessi.


Per la lista dei dati contenuti nel profilo SPID del cittadino, si rimanda al capitolo [3.2.2 Flusso di Registrazione](#), di queste linee guida.

Nel caso in cui il Service Provider abbia bisogno di ulteriori informazioni rispetto a quelle già ereditabili da SPID, le può richiedere successivamente alla login con SPID, utilizzando dei form. È severamente vietato richiedere all'utente di inserire manualmente informazioni che possono già essere estrapolate dal profilo SPID.

Nel caso in cui il Service Provider, per erogare il servizio a cui l'utente ha acceduto con successo con SPID, abbia bisogno di chiedere all'utente di accettare Termini e Condizioni Generali di Servizio, lo deve fare subito dopo l'accesso, in una schermata completamente dedicata allo scopo, che non ospiti altri elementi di fruizione del servizio, per non disorientare e distogliere l'attenzione dell'utente dalla call to action principale "Accetta le Condizioni per proseguire nel servizio".

Qualora i dati aggiuntivi per usufruire del servizio non siano immediatamente inseribili online da parte del cittadino (ad esempio, il cittadino deve caricare un documento di cui è sprovvisto al momento della login), il Service Provider è tenuto a spiegare in maniera comprensibile, perché il cittadino non può usufruire del servizio al momento, cosa è necessario e come il cittadino può procurarselo.

### 3.3.2 Procedure di Registrazione Assistita e Riutilizzo delle Identità Pregresse

 Questo paragrafo ha carattere normativo.

Tra febbraio e marzo 2018, AgID ha pubblicato le [determine](#) relative al processo di ottenimento dell'identità SPID semplificato, grazie al riutilizzo di dati provenienti da identità già esistenti presso i Service Provider che aderiscono al servizio.

In particolare le procedure sono due:

- la registrazione assistita, qui il [documento relativo](#);
- il riutilizzo delle identità pregresse di Service Provider accreditati, rilasciate successivamente a un riconoscimento di visu o identificazione informatica con livello di sicurezza equivalente o superiore al livello 2 di SPID. Qui il [documento relativo](#).

La registrazione assistita consiste nel riutilizzare i dati anagrafici dell'utente registrato presso il Service Provider A per pre-compilare il form di inserimento dei dati anagrafici durante il processo di registrazione, presso l'Identity Provider scelto dall'utente.

1. In questo caso il Service Provider A, che ha aderito alla procedura, notifica l'utente registrato e loggato riguardo la possibilità di registrarsi a SPID in maniera semplificata, tramite messaggi in bacheca, banner di comunicazione, oppure altri tipi di CTA inserite opportunamente nella UX del proprio canale.
2. L'utente interessato che clicca sul pulsante *Richiedi SPID*, viene reindirizzato a una pagina dove può visualizzare maggiori informazioni su SPID e sul flusso che sta per

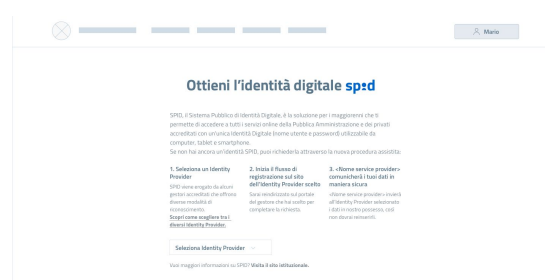
iniziare. Nella stessa pagina può scegliere l'Identity Provider che preferisce come gestore della sua identità SPID. In questa pagina è necessario inserire il link alla pagina <https://spid.gov.it/richiedi-spid>, per dare maggiori informazioni su come scegliere il proprio Identity Provider.

- Una volta selezionato l'Identity Provider, l'utente viene reindirizzato sul sito dell'Identity Provider, e precisamente alla pagina da cui parte il flusso di registrazione a SPID. Il sito dell'Identity Provider scelto, si apre in una nuova tab.
- Il Service Provider da cui è partito il flusso passerà i dati anagrafici dell'utente all'Identity Provider con il risultato che l'utente vedrà la maschera di inserimento dati prepopolata. I campi sono comunque tutti modificabili.
- Gli altri step della registrazione saranno esattamente gli stessi del flusso spiegato nella sezione [3.2.2 Flusso di registrazione](#).

Esempio di flusso di registrazione assistita:



F.23 - L'utente viene a conoscenza della procedura di registrazione assistita. In questo caso da un messaggio in bacheca [wireframe]



F.24 - L'utente è rediretto a una pagina dove ottiene maggiori informazioni [wireframe]



F.25 - L'utente viene rediretto all'inizio del flusso di registrazione presso l'Identity Provider che ha scelto [wireframe]

Il riuso delle identità pregresse riguarda i Service Provider che hanno rilasciato le proprie credenziali su riconoscimento *de visu* dell'utente o equivalente. Per poter iniziare il processo, l'utente deve effettuare un accesso con livello di sicurezza equivalente al livello 2 di SPID. Successivamente, il passo 1, 2, 3 riportati nel paragrafo precedente rimangono uguali, con un focus minore sulle differenze nella modalità di riconoscimento tra i diversi Identity Provider, dal momento che non è più necessario.

Una volta atterrati sulla pagina dell'Identity Provider, che si aprirà in una nuova tab, il flusso di registrazione sarà semplificato come segue:

L'utente deve:

1. Confermare i suoi dati anagrafici che verranno passati dal Service Provider in forma non modificabile (ed eventualmente aggiungere i dati mancanti)

2. Visualizzare e accettare le condizioni generali di servizio e della privacy
3. Scegliere le credenziali per l'account SPID

Il passaggio di riconoscimento non è più necessario perchè è da considerarsi assolto dal Service Provider che garantisce che l'identità dell'utente sia reale.

F.26 - Stepper di registrazione (lato Identity Provider) semplificato [wireframe]

I passaggi dei flussi indicati possono essere ordinati diversamente da quanto rappresentato qui a seconda delle esigenze dell'Identity Provider.

### 3.3.3 Deleghe

© Questo paragrafo ha carattere di raccomandazione.

Se il servizio erogato dal Service Provider lo richiede, SPID permette la creazione di una delega tra due utenti in maniera sicura. La condizione necessaria è che entrambi gli utenti siano in possesso di un'identità digitale SPID.

Tramite delega, l'utente A permette a un'altra persona (utente B) di operare per conto proprio all'interno di uno specifico servizio (o di un sottoinsieme di funzionalità del servizio).

Il flusso di creazione della delega è il seguente:

1. L'utente A effettua il login con SPID.
2. All'interno di un flusso di onboarding o nella pagina di profilo/impostazioni, l'utente clicca sul pulsante *Aggiungi delega* (label non vincolante).
3. In una nuova pagina viene chiaramente descritto quale potere si sta cedendo o condividendo e viene richiesto all'utente di inserire il nome, cognome e codice fiscale della persona che si vuole delegare.
4. A seconda della sensibilità e del rischio legato al servizio, si può terminare il flusso con una pagina di riepilogo e una semplice call to action di conferma, oppure richiedere una conferma più sicura richiedendo un livello 2 di SPID (codice di verifica temporaneo o autenticazione in app).

Esempio di flusso di delega in un servizio da app mobile:



F.27 - L'utente accede con SPID [wireframe]

F.28 - L'utente autorizza l'invio dei dati [wireframe]

F.29 - L'utente clicca sul pulsante Aggiungi Delega [wireframe]

Una volta avvenuto questo processo, l'utente B che accede al servizio con SPID riceverà una comunicazione per accettare o meno la delega ricevuta. A delega accettata, sarà cura del Service Provider permettere all'utente B di accedere alle funzionalità di cui è stato incaricato. Il Service Provider che permette la creazione di deleghe è tenuto a mostrare all'utente la lista delle deleghe create nella sua area personale, fornendo anche la possibilità di rimuoverle.

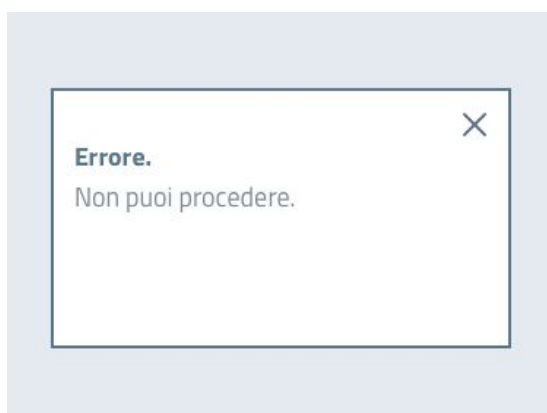
### 3.4 Errori e Notifiche di utilizzo

☞ Questo paragrafo ha carattere di raccomandazione.

Come specificato nel capitolo [2.2 Tone of voice e lingua](#), il testo è un ingrediente fondamentale per disegnare un'esperienza utente efficace.

Nei casi particolari di messaggi di errore o di notifiche si richiede di creare messaggi semplici, chiari e brevi che informino l'utente riguardo:

- Cos'è successo e perché: si devono evitare errori generici o eccessiva vaghezza. I messaggi devono fornire il giusto quantitativo di dettagli, ma senza entrare troppo nel tecnico per rimanere chiari e comprensibili a tutti.



F.33 - Esempio di errore generico e vago.



F.34 - Errore chiaro e "parlante".

- Cosa deve/può fare l'utente: dopo aver detto all'utente cos'è successo, suggerire un passo successivo, sia che si tratti di comunicare cosa può fare per risolvere un problema, di ricercare informazioni, ecc.

Esempio di una notifica di accesso:

*Hai effettuato un accesso al sito del Comune di Roma il giorno 20 marzo 2018 alle 19:08, via browser Safari.*

*Puoi visualizzare la lista dei tuoi accessi sull'app della tua identità SPID. Apri.*

*Non sei stato tu? Segnala l'anomalia al numero xxx xxxx.*

- Utilizzare il tono adeguato al contesto: quando si ragiona sul messaggio da esporre all'utente, si pensi alla situazione che ha generato il messaggio e alla situazione in cui si trova la persona. Ad esempio, utilizzare ironia o sarcasmo per quanto chiaro e amichevole sia il tono di voce suggerito per SPID, può aumentare la frustrazione dell'utente in caso di errore.
- Utilizzare il giusto formato di comunicazione: in linea direttamente in pagina, con un banner, messaggi SMS, e-mail, ecc.

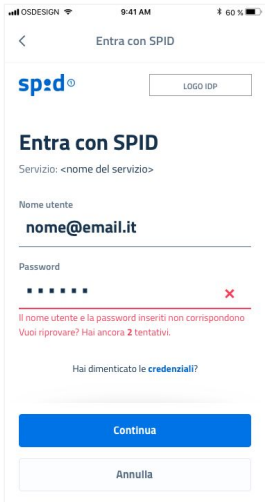
Scrivere messaggi chiari, semplici ed esplicativi può far apprezzare una notifica o ridurre la frustrazione degli utenti in caso di errore. Di seguito trovate una lista dei messaggi di errore o delle notifiche più comuni relative al servizio SPID, per prendere spunto.

### Errori

Gli errori possono essere mostrati in diversi formati a seconda della situazione in cui si verificano. I formati principali sono:



F.35 - Full page  
[grafica]



F.36 - In-line  
[grafica]



F.37 - Banner  
[proposta grafica]



F.38 - Banner + Pagina  
scelta identity provider  
[grafica]

Tipologia	Scenario	Formato	Chi mostra l'errore?	Messaggio	Error code*
System failure	Il servizio non risponde lato	Full page	IdP	Il servizio non risponde, ti invitiamo a riprovare.	SAML: 2,3  OIDC: server_error,

	Identity Provider			Se il problema persiste contatta l'assistenza clienti <descrizione canale servizio clienti>. <b>CTA:</b> Torna indietro.	temporarily_unavailable
System failure	La richiesta inviata dal Service Provider contiene degli errori	Full page	IdP	Non è al momento possibile accedere con SPID a questo servizio. Contatta l'assistenza clienti del servizio a cui stai provando ad accedere. <b>CTA:</b> Torna indietro.	SAML: 4-18  OIDC: invalid_client, invalid_request, invalid_scope
System failure	Il Service Provider ha riscontrato errori temporanei nella comunicazione con l'IdP	Banner/dialog	SP	Non è al momento possibile accedere con SPID a questo servizio. Riprova più tardi.	OIDC: temporarily_unavailable
System failure	Il Service Provider ha riscontrato errori nella lettura della risposta dell'IdP o nella comunicazione	Banner/dialog	SP	Non è al momento possibile accedere con SPID a questo servizio. Contatta il nostro servizio clienti: <descrizione canale servizio clienti>.	SAML: errori di lettura o verifica dell'asserzione.  OIDC: errori nelle chiamate dirette agli endpoint
User input	L'utente ha inserito le credenziali sbagliate	In linea	IdP	Il nome utente e la password inseriti non corrispondono. Vuoi riprovare? Hai ancora X tentativi.	SAML: 19
User input	L'utente ha inserito le	Full page	IdP	Hai inserito delle credenziali errate per più di X volte.	SAML: 19

	credenziali sbagliate per troppe volte			<p>Il tuo account è stato momentaneamente e bloccato. Per utilizzare la tua identità SPID, utilizza la procedura di sblocco.</p> <p><b>CTA:</b> Riattiva SPID / Torna indietro</p>	<p>OIDC: access_denied (Torna indietro)</p>
User condition	L'utente non è in possesso delle credenziali del livello necessario, perché il suo Identity Provider non le eroga	Pagina di scelta degli Identity Provider + Banner	SP	<p>Il tuo Identity Provider non fornisce il livello di autenticazione richiesto. Se hai un'altra identità SPID che lo fornisce, seleziona il relativo Identity Provider.</p> <p><b>CTA:</b> Annulla</p>	<p>SAML: 20</p> <p>OIDC: access_denied</p>
User condition	L'utente non è in possesso delle credenziali del livello necessario, ma il suo Identity Provider le eroga	Full page	IdP	<p>Al momento non possiedi lo strumento per effettuare questa operazione.</p> <p><b>CTA:</b> Scopri di più / Torna indietro.</p>	<p>SAML: 20</p> <p>OIDC: access_denied (Torna indietro)</p>
User condition	Per qualunque motivo l'utente non sia in possesso delle credenziali del livello necessario	Banner/ Dialog	SP	<p>Non è stato possibile terminare l'operazione.</p> <p>&lt;Se esistono delle soluzioni alternative che permettono all'utente di completare l'operazione, elencarle qui&gt;.</p>	SAML: 20

System condition	È scaduto il tempo limite per completare la procedura di accesso	Banner/Dialog	SP	La tua sessione è scaduta. Per continuare effettua nuovamente l'accesso. <b>CTA</b> (solo su dialog): Riprova / Torna indietro	SAML: 21
User input	L'utente nega il permesso al passaggio dei dati	Banner/Dialog	SP	Non è stato possibile completare l'operazione. Per continuare dai il consenso al passaggio dei dati. <b>CTA</b> (solo su dialog): Riprova / Torna indietro	SAML: 22  OIDC: access_denied (Torna indietro)
User condition	L'identità SPID dell'utente è sospesa/revocata	Full page	IdP	La tua identità SPID risulta sospesa o revocata. Per riattivare il tuo account, attiva la procedura di riattivazione. <b>CTA</b> : Riattiva / Torna indietro	SAML: 23  OIDC: access_denied (Torna indietro)
User input	L'utente clicca sul pulsante <i>Annulla</i> durante il flusso di accesso	Banner/Dialog	SP	Hai annullato l'operazione. Vuoi riprovare?	SAML: 24  OIDC: access_denied
User condition	La connessione internet non funziona	Full page	SP	Sei disconnesso. Controlla la tua connessione internet e riprova.	

\*I numeri degli errori SAML sono associati alle anomalie descritte nella [Tabella dei messaggi di anomalia di SPID](#). I codici degli errori OpenID Connect (OIDC) sono definiti nelle Linee Guida OpenID Connect.

### Notifiche (inviate dall'Identity Provider)

Scenario	Formato	Messaggio
Invio OTP dispositivo	SMS/Email	SPID <nome identità Identity Provider> - il tuo codice di verifica temporaneo è XXXXXX. Inseriscilo per proseguire l'operazione.
Notifica di accesso	SMS	Hai effettuato l'accesso a <nome del servizio> il giorno gg/mm/aaaa. Per visualizzare il registro completo dei tuoi accessi vai alla tua pagina di gestione account.
Notifica di accesso	E-mail	Ciao <nome utente>, Hai effettuato l'accesso a <nome del servizio> il giorno gg/mm/aaaa, via <nome del canale (es. browser Chrome, app mobile, ecc.)>. Per visualizzare il registro completo dei tuoi accessi vai alla tua pagina di gestione account. Non sei stato tu ad effettuare l'accesso? Contatta subito il servizio clienti <indicazioni canale servizio clienti>.

# 04 Risorse, Asset e Materiali

## Invio dei loghi e delle informazioni da parte degli Identity e Service Provider

👉 Questo paragrafo ha carattere normativo.

Si richiede agli Identity e Service Provider l'invio delle seguenti informazioni per poterle inserire, aggiornate, nelle interfacce:

- Nome Identity Provider / Service Provider / Attribute Provider
- Logo Identity Provider / Service Provider / Attribute Provider
- Nome del servizio che gestisce il servizio SPID (per Identity Provider)
- Logo del servizio che gestisce il servizio SPID (per Identity Provider)

I loghi dovranno essere inviati in formato vettoriale (eps).

E' responsabilità dell'entità comunicare all'indirizzo [spid@pcert.agid.gov.it](mailto:spid@pcert.agid.gov.it), tramite la pec e il referente segnalati nella convenzione stipulata, eventuali modifiche da apportare che saranno vagliate dal Referente AgID di SPID e quindi caricate sul Registro SPID. Eventuali difformità verranno comunicate tempestivamente al soggetto proponente.

### 4.1 Sito Ufficiale di SPID

❖ Questo paragrafo ha carattere informativo.

Il sito ufficiale di SPID è <https://spid.gov.it/>

Il sito è gestito interamente da AgID e dal Team per Trasformazione Digitale e rappresenta la fonte ufficiale e sempre aggiornata per reperire informazioni sul servizio.

Le linee guida emanate da AgID divengono efficaci dopo la loro pubblicazione nell'apposita area del sito internet istituzionale di AgID stessa.

### 4.2 Developers Italia

❖ Questo paragrafo ha carattere informativo.

[Developers Italia](#) contiene gli asset e le risorse applicative disponibili per facilitare l'implementazione di SPID, per Identity e Service Provider.



### 4.3 Sezione SPID AgID

❖ Questo paragrafo ha carattere informativo.

Sul sito di AgID sono disponibili le versioni ufficiali dei regolamenti attuativi, regole tecniche, linee guida e avvisi.

<http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid>

### 4.4 Piano Triennale

❖ Questo paragrafo ha carattere informativo.

Il Piano triennale è documentato sul sito: <https://pianotriennale-ict.italia.it/>

Il Piano Triennale per l'informatica nella Pubblica amministrazione è il documento di indirizzo strategico ed economico attraverso il quale viene declinato il Modello strategico di evoluzione del sistema informativo della Pubblica amministrazione. Nasce per guidare operativamente la trasformazione digitale del paese e diventa riferimento per le amministrazioni centrali e locali nello sviluppo dei propri sistemi informativi.

Definisce le linee guida della strategia operativa di sviluppo dell'informatica pubblica fissando i principi architetturali fondamentali, le regole di usabilità e interoperabilità, precisando la logica di classificazione delle spese ICT. Grazie al Piano si chiarisce il modello per lo sviluppo del digitale secondo cui:

- il livello nazionale definisce regole, standard e realizza piattaforme abilitanti che ottimizzano investimenti;
- le amministrazioni - centrali e locali - sviluppano servizi secondo le proprie specificità utilizzando competenze interne e/o di mercato;
- il privato, compresa la strategia di paese, programma investimenti di lungo periodo e sfrutta nuove opportunità di mercato creando soluzioni che si integrino con le piattaforme nazionali.

SPID compare tra le piattaforme tecnologiche abilitanti documentate nel piano triennale:

<https://pianotriennale-ict.italia.it/piattaforme-abilitanti/>

### 4.5 CAD

❖ Questo paragrafo ha carattere informativo.

Il [Codice dell'Amministrazione Digitale](#) è un atto legislativo della Repubblica Italiana. Costituisce un corpo organico di disposizioni che regola l'utilizzo dell'informatica come strumento privilegiato nei rapporti tra la Pubblica Amministrazione italiana e i cittadini. SPID è istituito dall'Art.64, comma 2-bis, della sezione III.