Al via dal 15 marzo Spid, il nuovo sistema di login per i servizi pubblici online

Un pass digitale e universale per dialogare con le p.a.

Pagine a cura
DI ANTONIO CICCIA MESSINA

Pin unico per i servizi con la Pubblica amministrazione. O meglio un'unica credenziale. Il sistema si chiama Spid (sistema pubblico di identità digitale) e parte il 15 marzo 2016 con una sperimentazione su larga scala.

Le prime amministrazioni che aderiscono sono l'Agenzia delle entrate, Inps, Inail, comune di Firenze, comune di Venezia, comune di Lecce, regione Toscana, regione Liguria, regione Emilia-Romagna, regione Friuli Venezia Giulia, regione Lazio e regione Piemonte. E InfoCert, Poste Italiane e Tim stanno rendendo disponibili le prime identità digitali.

L'idea è semplificare le modalità di fruizione telematica dei servizi, consentendo al cittadino di dialogare utilizzando una credenziale con tutti i soggetti coinvolti.

Vediamo cosa cambia per cittadini e imprese.

In dettaglio Spid è il nuovo sistema di login che permetterà a cittadini e imprese di accedere con un'unica identità digitale a tutti i servizi online di pubbliche amministrazioni e imprese aderenti. Grazie a Spid si può dire addio alle innumerevoli password, chiavi e codici necessari oggi per utilizzare i servizi online di p.a. e imprese. Tra i servizi fruibili con il sistema Spid possono elencarsi: servizi Anagrafici, 730 precompilato, incentivi alle imprese, certificazione Isee, iscrizione ad asili nido, domanda d'iscrizione alla gestione separata, sportello telematico Imu, Tari, Tasi, certificati energetici, pagamenti contributi Inps lavoratori domestici, invio domanda di disoccupazione, ritiro referti medici.

Altri servizi raggiungibili con il sistema Spid sono lo Sportello unico per le attività produttive (Suap), lo Sportello unico per l'edilizia (Sue) e la prenotazione tramite Cup. Inoltre in alcune regioni si prevede l'estensione all'accesso ad avvisi e bandi, al fascicolo sanitario, al bollo auto e ai servizi per lo studente.

L'identità Spid è costituita da credenziali con caratteristiche differenti in base al livello di sicurezza richiesto per l'accesso. Ci sono tre livelli di sicurezza, ognuno dei quali corrisponderà a tre diversi livelli di identità Spid.

Il primo livello si basa su sistemi di autenticazione informatica a un singolo fattore: per esempio l'autenticazione tramite identificativo utente (Id) e password scelta dall'interessato.

Il secondo livello di sicurezza prevede sistemi di autenticazione informatica a due fattori: per esempio tramite password e generazione di una One Time Password inviata dall'utente oppure l'invio di un sms, liste-tabelle predefinite o applicazioni mobili per smartphone o tablet collegati in rete. Infine il terzo livello è un sistema di autenticazione informatica a due fattori basati su certificati digitali e criteri di custodia delle chiavi private su dispositivi, come per esempio l'autenticazione combinata tramite password e una smart card.

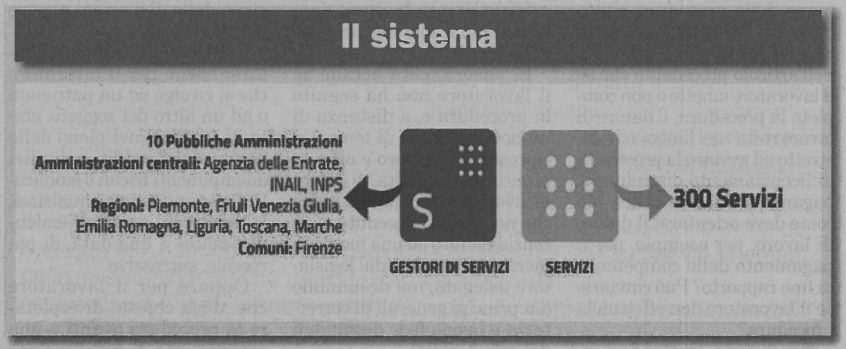
Pubbliche amministrazioni e privati definiranno autonomamente il livello di sicurezza necessario per poter accedere ai propri servizi digitali.

Le credenziali Spid garantiranno un accesso unico a tutti i servizi da molteplici dispositivi.

L'identità Spid viene rilasciata dai Gestori di identità digitale (Identity Provider), soggetti 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, il quale, dopo aver verificato i dati del richiedente, emette l'identità digitale rilasciando le credenziali all'utente. Ogni gestore può scegliere tra diverse modalità di verifica.

Il cittadino può scegliere il gestore di identità digitale che preferisce.



Previste forme di verifica

Le identità digitali rilasciate all'utente contengono obbligatoriamente il codice identificativo, gli attributi identificativi e almeno un attributo secondario.
Per codice identificativo si intende il particolare attributo assegnato dal gestore dell'identità digitale che consente di individuare univocamente un'identità digitale nell'ambito dello Spid.
Gli attributi identificativi, per le persone fisiche sono nome, cognome, luogo e data di nascita, sesso, codice fiscale, estremi di un valido documento d'identità, mentre per le persone giuridiche sono ragione o denominazione sociale, sede legale, codice fiscale o partita Iva, visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società e gli estremi del documento d'identità utilizzato dal rappresentante legale.
L'attributo secondario serve per le comunicazioni tra il gestore dell'identità digitale e l'utente. Gli attributi secondari sono il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale ed eventuali altri attributi individuati dall'Agid funzionali alle comunicazioni.
Per gli attributi secondari devono essere forniti almeno un indirizzo di posta elettronica e un recapito di telefonia mobile.
I gestori devono accertare che l'indirizzo di posta elettronica comunicato sia unico in ambito Spid, cioè non sia stato precedentemente indicato per l'acquisizione di un'identità digitale.
Infine sono attributi qualificati: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati.
Le identità digitali saranno rilasciate a domanda e si deve verificare l'identità fisica del soggetto richiedente, tramite esibizione a vista di un valido documento d'identità e, nel caso di persone giuridiche, della procura attestante i poteri di rappresentanza. In alternativa sono previste forme di verifica dell'identità informatica (per esempio mediante acquisizione del modulo di adesione allo Spid sottoscritto con firma elettronica qualificata o con firma digitale).
Una misura indirettamente precauzionale è quella che fa leva sull'aggiornamento costante delle informazioni (attributi identificativi) sul conto del titolare dell'identità. È, infatti, previsto l'obbligo degli utenti di informare tempestivamente il gestore dell'identità digitale di ogni variazione degli attributi previamente comunicati; e il gestore deve provvede tempestivamente ai necessari aggiornamenti.

Attualmente i gestori di identità digitale sono Poste italiane Id, Infocert Id e Tim Id.

Il sistema prevede alcune cautele contro l'utilizzo abusivo o fraudolento dell'identità digitale. A posteriori (dopo il furto di identità) si può agire civilmente per il risarcimento dei danni e si può denunciare penalmente: il codice penale prevede la reclusione fino a tre anni (oltre a una multa) per il gestore di identità (articolo 640-quinquies del codice penale).

In astratto potrebbe capitare anche che un service provider si inventi che un cittadino ha acceduto a un servizio ed effettuato determinate azioni dopo essersi autenticato con una identità Spid. Tuttavia, spiega l'Agid, differentemente dal caso in cui si utilizzasse una carta elettronica, con l'uso dell'identità Spid il reato (sostituzione di persona, frode informatica ecc.) sarebbe facilmente provabile. Il gestore dell'identità infatti deve mantenere traccia dei processi di autenticazione effettuati.

Le misure precauzionali adottate sono le seguenti. Se il cittadino o l'impresa ritiene che la propria identità digitale sia stata utilizzata abusivamente o fraudolentemente da un terzo, potrà bloccare l'identità digitale, chiedendone la sospensione al gestore della stessa e, se conosciuto, anche al fornitore di servizi presso il quale essa risulta essere stata utilizzata.

Se la richiesta sarà inviata con posta elettronica certificata, o sottoscritta con firma digitale o firma elettronica qualificata, il gestore dell'identità digitale e il fornitore di servizi eventualmente contattato provvederanno subito; negli altri casi si procederà previa verifica della provenienza della richiesta di sospensione da parte del soggetto titolare dell'identità digitale.

La sospensione durerà un massimo di 30 giorni, decorsi i quali l'identità digitale dovrà essere ripristinata o revocata. La revoca scatta quando il gestore avrà ricevuto dall'interessato copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è stata basata la richiesta di sospensione.