ItaliaOggi Sette

Data 14-03-2016
Pagina 4/5
Foglio 1 / 4

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.

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.

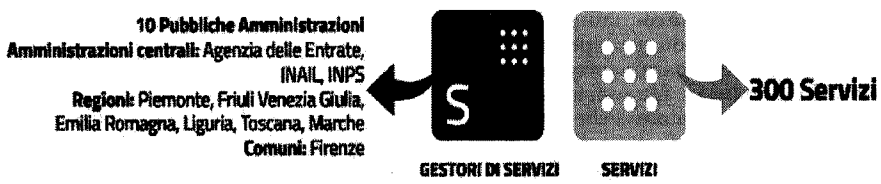
Se la richiesta sarà inviata con posta elettronica certificata, o sottoscritta con firma digitale o firma elettronica qualificata, il gestore dell'identità digitale e il fornitore di servizi eventualmente contattato provvederanno subito; negli altri casi si procederà previa verifica della provenienza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

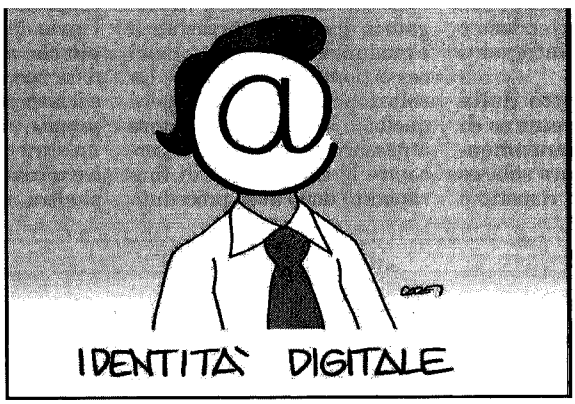
La sospensione durerà un massimo di 30 giorni, decorsi i quali l'identità digitale dovrà essere ripristinata o revocata. La revoca scatta quando il gestore avrà ricevuto dall'interessato copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è stata basata la richiesta di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

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.

Il sistema





Obiettivo 6 milioni di utenti

Sei milioni di identità digitali entro il 2016. È l'obiettivo fissato dall'Agid, anche se il primo bilancio andrà fatto a fine 2017. E a costo zero per il Pin relativo ai primi due livelli di sicurezza, che corrispondono alle versioni con cui si può accedere a tutti i servizi online.
Vediamo come si sono organizzati gli identity provider.
Tim Id mette a disposizione dal 15 marzo 2016 il set unico di credenziali, di accedere online a centinaia di servizi pubblici e privati sostituendo I precedenti codici.
In particolare, Tim Id potrà essere richiesto gratuitamente da tutti i cittadini effettuando la registrazione sul portale www.nuvolastore.il e seguendo la procedura di attivazione indicata. L'utente riceverà le credenziali Tim Id via email e sms.
Tim Id sarà utilizzabile su tutti i portali delle pubbliche amministrazioni locali e centrali e delle aziende private aderenti che esporranno l'Icona del lucchetto «Spid». Sono previsti livelli di sicurezza differenziati in base alle diverse tipologie di servizi cui si vuole accedere: l'accesso ai servizi informativi sarà consentito tramite nome utente e password stabiliti dall'utente stesso; per alcune operazioni, ove richiesta una maggiore sicurezza e tutela dei dati, sarà inviato all'utente un codice utilizzabile una sola volta (One Time Password) per completare l'accesso ai servizi.
Saranno inoltre disponibili un cruscotto di controllo e un servizio di notifiche sull'utilizzo della propria identità digitale Tim Id.
Il servizio potrà essere richiesto anche dalle aziende che avranno a disposizione, in opzione, identità multiple per i propri rappresentanti.
Un potenziale di 4 milioni di clienti di Poste Italiane potrà usufruire dello Spid, il sistema pubblico per l'identità digitale di cui il gruppo. Anche per PosteId il sistema parte dal 15 marzo 2016 e sarà reso disponibile al pubblico partendo dai clienti dotati di strumenti di riconoscimento in rete, e dai primi 396 uffici locali, con Venezia capofila.

Adesione obbligatoria per gli enti

Spid obbligatorio per le p.a. Per gli enti pubblici l'adesione al sistema pubblico di identità digitale è vincolante. Mentre per le imprese l'adesione allo Spid per fornire i propri servizi in rete è facoltativo. Lo precisa la circolare 7 del 22 febbraio 2016 di Assonime, dedicata all'illustrazione della novità in materia di digitalizzazione dei servizi. La circolare richiama, comunque, le disposizioni del codice dell'amministrazione digitale, in base alle quali l'impresa, che aderisce allo Spid per la verifica dell'accesso ai servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente, non è tenuta a un obbligo generale di sorveglianza delle attività sui propri siti ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70, sul commercio elettronico.
Invece, per gli enti pubblici, erogatori di servizi online, per i quali è necessaria l'identificazione informatica dell'utente, la normativa prescrive l'obbligo di consentire l'identificazione degli utenti mediante lo Spid.
Le p.a., pertanto, hanno l'obbligo di aderire allo Spid.
Le p.a., inoltre, hanno 24 mesi di tempo, decorrenti dalla data di iscrizione nel registro Spid del primo gestore di identità digitale, per adeguare i sistemi di login dei propri siti all'accesso tramite Spid.
La circolare Assonime ricorda che le pubbliche amministrazioni possono anche affidare ai gestori di identità dello Spid le funzioni di autenticazione informatica e che le pubbliche amministrazioni in qualità di fornitori di servizi possono utilizzare a titolo gratuito le verifiche effettuate dai gestori di identità digitale e dai gestori di attributi qualificati.
Le p.a., infine, devono trattare i dati nel rispetto della disciplina sulla protezione dei dati personali: in particolare i fornitori di servizi devono informare l'utente che l'identità digitale e gli eventuali attributi qualificati saranno verificati rispettivamente presso i gestori dell'identità digitale e i gestori degli attributi qualificati.

ItaliaOggi Sette

Data 14-03-2016
Pagina 4/5
Foglio 4 / 4

La privacy non è a rischio

Non ci sarà nessuna profilazione a scopi commerciali dei dati dell'utente da parte degli Identity Provider.

Inoltre il sistema Spid protegge i dati personali più di una smart-card. Con le carte elettroniche i dati personali utili a verificare l'identità in rete sono tutti disponibili al service provider.

Con Spid, sebbene l'utente sarà sempre autenticato con assoluta certezza, saranno forniti al service provider, previa autorizzazione dell'utente, solo i dati strettamente necessari per la specifica transazione. Per esempio, per i servizi che necessitano solo di verificare la maggiore età del soggetto o di conoscere un indirizzo email, l'identity provider fornirà al service provider solo le informazioni strettamente necessarie.

In corso d'opera, tra l'altro, il Garante della privacy ha fornito le sue osservazioni (provvedimento n. 660 del 17 dicembre 2015), chiedendo una rete di garanzie, tra le quali: stringenti controlli dell'Agid in tema di sicurezza informatica e protezione dei dati; una più puntuale definizione delle modalità di conservazione della documentazione inerente la creazione e il rilascio dell'identità digitale; la specificazione delle caratteristiche del servizio all'utente dell'avvenuto utilizzo delle sue credenziali; una migliore esplicitazione delle procedure di sospensione e revoca dei gestori. È stata inoltre sancita la collaborazione tra Agid e Garante privacy con l'obiettivo di vigilare sul funzionamento di un sistema così delicato.

Il garante ha anche chiesto di specificare che, se il gestore dell'identità digitale fornisce solo l'identificazione da remoto come modalità per la verifica dell'identità del richiedente, ciò deve essere messo in evidenza, oltre che nelle condizioni e termini del contratto, anche nell'informativa da rendere all'utente.

Sempre a protezione dei dati bisogna ricordare l'obbligo per il gestore di comunicazione di eventuali violazioni o intrusioni nei dati personali (i cosiddetti data breach) e le procedure che l'Agid è tenuta ad adottare in caso di inadempimenti del gestore.

Si potranno avere più identità Spid, senza che questo provochi intoppi. Sul sito dell'Agid è trattato il caso del cittadino dotato di due identità Spid fornite da due diversi gestori, che inizi un procedimento amministrativo con una identità Spid, e pone il quesito se quel cittadino dovrà ricordarsi quale identità ha utilizzato per accedere nuovamente a quella p.a. per seguire la propria pratica o presentare altra documentazione. La risposta è negativa, in quanto l'ufficio pubblico, sarà in grado di riconoscere il cittadino e consentirgli di accedere ai propri dati e alle proprie pratiche a prescindere dall'identità Spid utilizzata dal cittadino.

Il cittadino non dovrà temere di avere dimenticato una identità digitale. Non si corre il rischio di avere identità digitali attive di cui si perda memoria. Le norme, infatti, prescrivono al gestore dell'identità di tener traccia dell'uso delle singole identità emesse e, non rilevandone l'utilizzo per un periodo di 24 mesi, deve revocare l'identità non utilizzata.

Per l'uso dell'identità Spid, tra l'altro, non sarà obbligatorio l'uso di alcun lettore di carte ma potrà essere utilizzata in diverse modalità (per esempio, pc, smartphone, tablet ecc.). Il cittadino sarà libero di scegliere la soluzione che offre il mercato e cambiarla quando vuole.

Una volta scelto un gestore di identità e ottenuta l'identità, il cittadino non sarà vincolato a quel gestore, in quanto potrà revocare l'identità ottenuta in qualunque momento senza dover fornire alcuna motivazione.

I tre livelli di sicurezza

spid 1 — Identità SPID di primo livello. Ad es. permette l'autenticazione tramite ID e password stabilita dall'utente

spid 2 — Identità SPID di secondo livello. Ad es. permette l'autenticazione tramite password + generazione di una One Time Password inviata all'utente

spid 3 — Identità SPID di terzo livello. Ad es. permette l'autenticazione tramite password + smart card

I vantaggi

Semplificazione	Un unico login per accedere ai servizi,
	PA e imprese non dovranno più gestire fase autenticazione utenti
Sicurezza	Protezione garantita dei dati
	Nessuna profilazione dell'utente
Risparmio	Scompaiono gli oneri per la conservazione dei dati
	Si esternalizza la procedura di registrazione degli utenti

Fonte: Agid - Agenzia per l'Italia Digitale