SPID – Sistema Pubblico di Identità Digitale - è il nuovo sistema di autenticazione che permette a cittadini e imprese di accedere ai servizi online della PA e dei privati aderenti, in modalità sicura e garantita, da computer, tablet e smartphone.

I servizi abilitati attraverso SPID
Dal pagamento delle tasse ai servizi sanitari, passando per i servizi Inps e Inail, sono molteplici i servizi della Pubblica Amministrazione a cui si può già accedere tramite Spid: dal pagamento della Tasi al bollo auto, dalle prestazioni sanitarie al fascicolo dell'Inps, dal riscatto della laurea, richiesta degli assegni familiari, dalla consultazione Cud, alla richiesta bollettini, dal saldo di tributi regionali, al pagamento delle mensa scolastica e ticket sanitari via web. A questi servizi si aggiungono tutti i servizi per le persone giuridiche e i liberi professionisti.

I veri vantaggi di SPID
I Service Provider che aderiscono allo SPID, sia Pubbliche Amministrazioni sia imprese private, possono disporre di un parco utenti senza censirli, non avranno gli oneri derivanti dalla conservazione dei dati personali, non dovranno preoccuparsi di evitare attacchi volti al furto delle credenziali. Inoltre, i Service Provider possono avere profili con un'identità certa, eliminando i cosiddetti "falsi profili", ed univoca, eliminando i duplicati.
Per gli utenti, SPID consente di semplificare la vita di cittadini e imprese nell'interazione con la Pubblica Amministrazione tramite servizi online grazie ad un unico login. Il sistema garantisce la massima sicurezza e privacy. SPID assicura la massima riservatezza dei dati ed è pensato proprio per aumentare la trasparenza sulla gestione dei propri dati ed erogare servizi secondo il principio dei dati minimi. Il Service Provider non può conservare i dati dell'utente che riceve dall'Identity Provider ed è assolutamente vietata la tracciatura delle attività di un individuo.

I livelli di sicurezza per la propria identità digitale:
Il modello SPID per il Sistema Pubblico di Identità Digitale prevede 3 livelli di sicurezza.

- **Livello 1 *(userID e password)*** garantisce con un buon grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio moderato e compatibile con l'impiego di un sistema autenticazione a singolo fattore, ad es. la password; questo livello può essere considerato applicabile nei casi in cui il danno causato, da un utilizzo indebito dell'identità digitale, ha un basso impatto per le attività del cittadino/impresa/amministrazione. Per il livello 1 la credenziale sarà dunque una password di almeno 8 caratteri, da rinnovarsi ogni 180 giorni, formulata secondo i consueti criteri di sicurezza.
- **Livello 2 *(userID, password + ulteriore fattore di autenticazione)*** garantisce con un alto grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio ragguardevole e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell'identità digitale può provocare un danno consistente. Per il livello 2, oltre alla password sarà necessario

inserire il codice proveniente da un dispositivo a chiave variabile (c.d. One Time Password) che potrebbe essere anche un'applicazione sul cellulare.

- **Livello 3 *(userID, password + ulteriore fattore di autenticazione basato su certificati digitali)*** garantisce con un altissimo grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio altissimo e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su altri dispositivi; questo è il livello di garanzia più elevato e da associare a quei servizi che possono subire un serio e grave danno per cause imputabili ad abusi di identità; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell' identità digitale può provocare un danno serio e grave.

Gli identity provider nello SPID

Gli attori che possono assumere il ruolo di Identity Provider sono molteplici (banche, operatori di telefonia mobile, certification authority, fornitori di soluzioni IT) e giocano un ruolo fondamentale nel decretare il successo del sistema perché portano in "dote" allo SPID il proprio bacino di utenti potenziali. Ad oggi, febbraio 2018, sono nove gli Identity Provider che hanno richiesto e ottenuto la certificazione da parte dell'AgID: Aruba, Infocert, Intesa (Gruppo Ibm), Lepida, PosteItaliane (PosteID), SielteID, Telecom Italia Trust Technologies, Namirial, Register.it.

Quali attori e ruoli prevede SPID, e chi lo può utilizzare

Lo SPID identifica differenti ruoli:

- Gestori dell'identità digitale (o Identity Provider), sono imprese private accreditate allo SPID (ottengono la "licenza" da AgID) con il compito di identificare l'utente in modo certo, di creare le identità digitali, di assegnare le credenziali, di gestire gli attributi degli utenti. Essi inoltre, in qualità di gestori di servizio pubblico, forniscono i servizi a pubbliche amministrazioni e imprese private aderenti di identificazione degli utenti, garantendo la correttezza dell'identità digitale e la riservatezza delle informazioni.
- Fornitori di servizi (o Service Provider) sono i soggetti privati e le Pubbliche Amministrazioni che erogano servizi online, per la cui fruizione è richiesta l'identificazione e l'autenticazione degli utenti.
- Utente: persona fisica o giuridica, titolare di un'identità digitale SPID, che utilizza i servizi erogati in rete da un fornitore di servizi, previa identificazione informatica.
- Agenzia è l'organismo di vigilanza che si occupa di gestire l'accreditamento e di monitorare i gestori dell'identità digitale e i gestori degli attributi qualificati.
- Gestori di attributi qualificati sono soggetti che hanno il potere di attestare gli attributi qualificati su richiesta dei fornitori di servizi.

Un utente si registra al servizio tramite un Identity Provider che crea un'identità digitale e gli assegna le credenziali per il riconoscimento. L'utente può utilizzare la sua identità digitale per l'accesso ai servizi online offerti dai Service Provider, che sono collegati a tutti gli Identity Provider. Sarà compito dell'Identity Provider verificare la correttezza dei dati di login immessi dall'utenti e fornire al Service Provider solo gli attributi dell'utente strettamente necessari alla fornitura del servizio.

Servizi disponibili con SPID

Servizi INAIL, Ambiente, Edilizia, Servizi INAIL Servizi di pagamento, Controllo Pagamenti, Tasse e Tributi, Visure, Controllo e Consultazione dati, Economia e finanze, Anagrafe, Fatturazione elettronica, Finanziamenti, Invio e richiesta documenti, Servizi INPS, Servizi di Certificazione e Autocertificazione, Servizi di pagamento, controllo pagamenti e tanto altro ancora.

Perché La Camera di Commercio?
Da dieci anni è punto di riferimento di imprese e professionisti sul fronte dell'identità digitale-Oggi questo patrimonio di esperienze è a disposizione della nuova piattaforma del sistema Paese. Inoltre puoi contare sull'aiuto e l'assistenza degli operatori di Sportello della Camera di Commercio e per qualunque dubbio o necessità hai delle persone preparate a cui rivolgerti.

Per saperne di più:

CONSULTA LE FAQ >>
SPID – Sistema Pubblico di Identità Digitale
E-mail: registro.imprese@molise.camcom.it