Domande Frequenti (FAQ) su

(A cosa serve SPID, come è fatto e perché, spiegato alla mia famiglia)

A cosa serve questa guida/FAQ?

Nel 2013 fui eletto in parlamento e proposi il sistema che oggi è SPID.
Mia moglie ha pensato di farsi un account SPID per accedere al fascicolo sanitario e qualche altro servizio. Mi ha chiesto di spiegarle come funziona e il perché di certe cose che le sembravano complicazioni inutili (ad esempio perché usare un generatore di codici sul cellulare – "autenticazione a due fattori").
Dopo che le ho spiegato tutto, rispondendo alle sue domande, ho provato a vedere online se c'era una simile guida/FAQ e non ho trovato nulla che rispondesse a tutto.
E allora, di getto, ho scritto queste FAQ che ho integrato anche con qualche domanda giuntami su twitter. (se avete altre domande, scrivetele pure nei commenti).
Spero vi sia utile!
(Potete farmi ulteriori domande, segnalarmi errori, imprecisioni o quant'altro sul mio blog all'indirizzo https://blog.quintarelli.it)

Stefano Quintarelli
twitter: @quinta

Indice delle domande

A cosa serve SPID?

SPID serve a farsi riconoscere con valore legale da un servizio online della Pubblica Amministrazione e/o di privati e ad accedere ai servizi pubblici online degli altri Stati UE. Di per sé non è un documento d'identità ma quando la Legge impone alla Pubblica Amministrazione di controllare il documento d'identità di chi accede a un servizio, identificarsi con SPID equivale anche a presentarlo.

Perché è utile?

Perché per accedere a determinati servizi online, in particolare quelli della PA, ma anche dei privati che forniscono servizi regolati dalla Legge, non è sufficiente fornire nome e cognome ed abbinare a questi un numero di telefono/email. Chiunque potrebbe disporre di questi dati. Chi fornisce il servizio deve accertarsi dell'identità del richiedente prima di poter dare l'accesso e dar corso alle richieste del cliente. Questa la ragione per cui la banca o la compagnia telefonica, ad esempio, vuole riconoscerci con un documento di identità.

Nella pubblica amministrazione, prima di SPID, per accedere ad un servizio online, serviva una smartcard (la tesserina di plastica tipo tessera sanitaria) con un pin/password. Una cosa macchinosa sia nella fornitura che nell'uso. Dove abito io la tessera sanitaria veniva spedita a casa, poi si doveva andare all'ASL a farsi riconoscere e a farsi consegnare un pezzo di codice e poi ti arrivava per posta un altro pezzo di codice e solo allora si poteva iniziare l'uso. Per usare questo tipo di carta però avevi bisogno di un lettore di smartcard (che praticamente nessuno aveva).

I servizi erano pochissimi e scarni perché gli utenti erano pochi. Ed è anche vero che gli utenti rimanevano pochi perché c'erano pochissimi servizi. Il lettore di tessere e la procedura di fornitura erano degli ostacoli che scoraggiavano quasi tutti (la provincia di Trento è l'eccezione che conferma la regola).

Per l'amministrazione non si tratta solo di fornire le credenziali. A volte gli utenti le perdono (o le persone muoiono) e quindi vanno revocate. Riconoscere a vista la persona, fornire le credenziali, gestire le loro sospensioni e revoche, il tutto per tutti i cittadini, è una attività costosissima per una pubblica amministrazione o un privato che voglia fornire un servizio online.

Tanti servizi pubblici sono gestiti con dei computer e dei database e sarebbero candidati ideali per essere messi online. Un motivo rilevante per cui non sono ancora erogati online al pubblico è proprio perché gestire il rilascio e la sicurezza delle credenziali specifiche per ogni servizio avrebbe un costo proibitivo, per cui il gioco non vale la candela.

Facevo sempre un esempio per chiarire: molti di noi hanno la tomba dei propri cari in un comune di origine e lì ci sono spese da sostenere e talvolta, esumazioni. Questi dati stanno all'interno di un piccolo server, ma non avrebbe senso renderli accessibili online perché gestire il "ciclo di vita" delle credenziali avrebbe un costo incredibilmente sproporzionato.

Il costo di rilasciare e mantenere in vita credenziali informatiche è infatti estremamente elevato e di fatto si giustificava solo quando erano in ballo servizi critici quali la sanità o la giustizia.
Ecco dunque l'idea: mettere a fattor comune il costo di gestione delle credenziali informatiche, così da abilitare la realizzazione e pubblicazione online pressoché di qualsiasi servizio.
Questo è SPID: un sistema di autenticazione che consente ad ogni amministrazione di concentrarsi sui servizi che deve erogare e non sulla gestione delle credenziali.
Ma non solo.
Desideriamo tutti che la pubblica amministrazione non ci chieda più informazioni che ci riguardano che essa abbia già in suo possesso. Molto più facile a dirsi che a farsi. Sia per questioni di privacy che per correttezza dei dati contenuti nei database sia perché i database non usano criteri omogenei.
Se andiamo all'università, la chiave di accesso ai database è il numero di matricola, se andiamo in comune il numero di carta di identità, alla motorizzazione il numero della patente, all'ospedale il numero di tessera sanitaria, all'agenzia delle entrate il codice fiscale, e via dicendo.
Rendere accessibili tutti i servizi usando come chiave di accesso il codice fiscale spinge tutte le amministrazioni a creare un substrato comune, una fondamenta per riconoscere quali documenti ci riguardano, in ogni amministrazione. Per inciso SPID, consentendo di identificare le persone, potrà anche consentire a ciascuno (se lo vorrà) di autorizzare un terzo ad accedere a proprie informazioni, superando così anche problemi di privacy nell'accesso ai documenti della PA che ci riguardano.

Ho sentito che è difficile ottenere SPID. È vero?

SPID richiede alcuni controlli sull'identità della persona che deve essere riconosciuta, di persona o a distanza, da un addetto prima che le credenziali siano emesse.
Questo avviene perché c'è bisogno di fiducia e perché SPID garantisce il riconoscimento delle persone e quindi le credenziali non possono che essere rilasciate dopo aver attentamente verificato l'identità di chi le richiede (con i suoi documenti di identità). In questo modo, poi, tutti i servizi online potranno fidarsi che chi usa quelle identità è realmente chi dichiara di essere.
Il fatto che sia estremamente facile registrarsi ai servizi online ci deve far riflettere sulla affidabilità con cui gli stessi ci identificano. In molti servizi chiunque può dichiarare dati anagrafici non corretti e registrarsi senza particolari verifiche. Basterebbe fare una ricerca online per trovare immagini di carte di identità da prendere, crearsi un indirizzo mail corrispondente e poi spacciarsi per qualcun altro.
SPID si basa invece su una verifica de visu di documenti di identità forniti dallo Stato (unico che può rilasciarli) su cui si poggia un servizio di erogazione e autenticazione/verifica delle credenziali. Questo servizio di autenticazione può essere fornito da amministrazioni pubbliche o

da privati, in conformità con le regole europee e come già avviene, ad esempio, per la posta elettronica certificata o per la firma digitale.
Con SPID si può accedere infatti (anche) a servizi che gestiscono dati assai privati e che consentono di disporre azioni per cui è necessario essere certi dell'identità del richiedente (pur senza chiedergli di andare presso uno sportello di un ufficio) ad esempio istanze che riguardano i diritti della persona, pagamenti, accessi a procedure amministrative.
Per questo SPID ha tre livelli di "fiducia" crescente, dal solito username/password adatto per i servizi più semplici (livello 1), ad un sistema di "autenticazione forte a due fattori" (livello 2) ad un sistema che sfrutta una smartcard (livello 3).
È dunque imprescindibile e necessario, al rilascio, fare una verifica approfondita, con controlli dietro le quinte, per accertarsi che chi richiede una credenziale sia effettivamente chi dice di essere. Sono verifiche simili a quelle che dovrebbero avvenire ad uno sportello, ma da remoto, ed una volta per tutte. E per questo fornire dichiarazioni false è un reato. (proprio per i controlli di sicurezza dietro le quinte le credenziali non sono rilasciate in tempo reale)
[Se vuoi saperne di più, vedi la sezione su "Cos'è la autenticazione a più fattori e perché serve?"].
Ciò detto, essendo il servizio erogato da più fornitori, come sempre quando si è in concorrenza ce n'è qualcuno più bravo degli altri. Se uno non ci soddisfa, possiamo sceglierne un altro. È il bello della concorrenza. [Vedi anche "Possiamo avere credenziali con più fornitori di servizi di autenticazione?"]
Ricordiamoci comunque che le procedure di rilascio vanno fatte una volta sola, dopodiché SPID ci identificherà per molti anni solo con pochi clic all'accesso ai servizi, garantendo la nostra identità.
Ottenere SPID non è certamente più complicato che richiedere la carta di identità o il passaporto, cosa che tutti, prima o poi, siamo chiamati a fare, anzi, è certamente più semplice.

Ho sentito che usare SPID è macchinoso. È vero?

Usare SPID certamente richiede un minimo di familiarità con l'uso dello smartphone o browser web e le relative procedure.
Il sistema effettua più verifiche ai livelli di sicurezza più elevati e questo può rendere l'uso in certi casi più complesso, ma comunque esso rimane piuttosto simile all'uso dei PIN e delle APP da tempo presenti sui sistemi di home banking. Premesso che, essendo il servizio erogato da più operatori, come sempre quando si è in concorrenza ce n'è qualcuno più bravo degli altri. Se un fornitore di SPID non ci soddisfa, possiamo sceglierne un'altro. È il bello della concorrenza.
In realtà, il sistema è meno macchinoso di quanto possa apparire, se capiamo il senso di ciò che facciamo.
Nella sezione "Perché è utile" spiego che SPID consente di mettere a fattor comune le credenziali, per accelerare lo sviluppo di servizi e favorire la realizzazione di sistemi di scambio di

documenti tra le amministrazioni. Ciò significa che l'amministrazione del Comune PIPPO che ci eroga servizi online per lo scuolabus delega al gestore di SPID la verifica delle nostre credenziali: Andiamo sul sito del Comune PIPPO, scegliamo il servizio scuolabus e clicchiamo "accedi con SPID" per passare temporaneamente al nostro gestore SPID che verifica le nostre credenziali e, se la verifica è positiva, il nostro gestore comunica al comune PIPPO alcuni dati identificativi (dopo avercene chiesto il permesso per rispettare la privacy).
Questo gestore SPID, che verifica le nostre credenziali, è il soggetto (privato o pubblico) cui ci siamo rivolti per ottenere le credenziali. È chiamato "identity provider" (ci fornisce il servizio di verifica dell'identità).
Quindi il flusso è
Comune PIPPO → "Identity Provider" SPID → Comune PIPPO
Solitamente la verifica fatta dall'Identity Provider prevede una autenticazione a più fattori, per maggiore sicurezza, simile a quella che facciamo in banca.
[Se vuoi saperne di più, vedi la sezione su "Cos'è la autenticazione a più fattori e perché serve?"].

Cos'e' un identity provider, un service provider, AgID, ecc.?

I soggetti SPID appartengono a quattro categorie:

- gli **utenti** (cittadini, imprese)
- i **gestori** che rilasciano le credenziali ed erogano il servizio di autenticazione ("identity provider" o IdP)
- i **fornitori** che erogano servizi online ("service provider"o SP) che autenticano gli utenti presso gli identity provider
- i **fornitori di attributi** ("attribute provider") che attestano una qualche informazione relativa ad una persona (ad esempio potranno esserlo le università che attestino la laurea o gli albi professionali per attestare l'iscrizione, ecc.).

Inoltre, strada facendo (non c'era nell'idea originaria), è stata aggiunta la figura degli "aggregatori" che sono sostanzialmente degli intermediari: se un soggetto vuole delegare a terzi l'offerta di propri servizi con accesso tramite SPID, può rivolgersi a un aggregatore. Si pensi ad esempio alle Regioni che erogano servizi per conto di molti piccoli comun. Così possono divenire service provider SPID delegando loro tutta l'attività.
Sia gli identity provider (IDP) che i service provider (SP) che gli attribute provider possono essere soggetti pubblici o privati.
Per IDP ed SP, oltre alle leggi normali sotto a vigilanza della magistratura ed alle norme sulla privacy sotto la vigilanza del Garante per la Privacy, è previsto un accreditamento ed una vigilanza svolta dall'Agenzia per l'Italia Digitale (con sanzioni pesanti, che possono arrivare fino a multe salatissime ed alla revoca dell'accreditamento, oltre ad altre sanzioni civili ed – eventualmente - penali)

Gli identity provider ad oggi sono 9, che cooperano in una sorta di federazione [link]

C’è solo Poste per avere SPID?

No. Poste, con la capillarità degli uffici postali, è il più diffuso, ma ci sono altri fornitori che svolgono le attività di riconoscimento e rilascio delle credenziali, anche online.
Ad oggi ci sono 9 fornitori, indicati qui [link]

Quali sono i dati raccolti da SPID?

In sostanza sono quelli che determinano il codice fiscale.
Essendo basato sull’identità certificata dallo Stato, è necessario un documento valido (carta di identità, passaporto, patente) per i dati anagrafici.
Anche se raro, si può verificare la cosiddetta “omocodia”, ovvero due persone diverse con stesso nome nate nella stessa città lo stesso giorno.
Queste due persone potrebbero avere il codice fiscale identico, per cui la situazione si risolve in sede di erogazione del codice fiscale. Per questo è richiesto anche il codice fiscale indicato sul tesserino del codice fiscale o sulla tessera sanitaria. Tutti questi dati che compongono il codice fiscale vengono mantenuti.
Inoltre viene richiesto un numero di cellulare ed un indirizzo email che servono come punti di contatto nella consueta procedura di attivazione di un servizio web.
Questi dati, mantenuti dal gestore dei servizi di autenticazione che hai scelto, non vengono forniti a terzi, se non su esplicita autorizzazione dell’utente.
Non possono essere forniti a terzi perché tutto il sistema è vigilato dal Garante della Privacy. Inoltre, se quando accediamo ad un fornitore di servizi questi richiedesse informazioni eccessive, non necessarie per effettuare il servizio, il trattamento sarebbe “non proporzionale” e può essere segnalato al Garante Privacy

Cos'è la autenticazione a più fattori e perché serve?

SPID ha tre livelli di “fiducia” crescente, dal solito username/password adatto per i servizi più semplici (livello 1), ad un sistema di “autenticazione forte a due fattori” (livello 2) ad un sistema che sfrutti un dispositivo fisico, come una smartcard (livello 3).
È divenuta prassi, anche se non è strettamente necessario, che le amministrazioni che erogano servizi chiedano una autenticazione a due fattori, come quella in uso per i servizi bancari. In realtà, per molti servizi a bassa criticità potrebbe essere sufficiente il semplice username/password ed infatti la normativa lo consente.

L'autenticazione "a due fattori" si chiama così perché oltre ad avere un fattore di sicurezza (la password) prevede l'uso di un ulteriore fattore di sicurezza. Di solito si parla di fattori di sicurezza "cosa sai" (la password), "cosa hai" (un oggetto fisico), "chi sei" (controllo biometrico).
La sola password può essere indovinata, scoperta, copiata, etc... e quindi un malintenzionato può impersonarci quindi "rubandoci l'identità".
Abbinando anche il controllo di un oggetto fisico (una volta erano delle specie di portachiavi che generavano un PIN) la probabilità di impersonazione è molto più bassa, basta che custodiamo con cura tale oggetto.
Oggi pressoché tutti abbiamo uno smartphone che assolve il ruolo di fattore "cosa hai". Una volta lo si faceva ricevendo un SMS con un codice, ora tipicamente il codice viene generato con una app presente sullo smartphone. Va detto che nel tempo il canale SMS è divenuto meno sicuro (non è impossibile intercettare SMS).
Ma è anche possibile perdere il cellulare e, se non si è messo un PIN di blocco, chi lo trovasse avrebbe accesso diretto alla app di generazione del codice di autenticazione a due fattori! Per questo, frequentemente, le app (ad esempio bancarie) che generano il codice di autenticazione a due fattori richiedono un PIN di sblocco. È il caso anche delle App di autenticazione a due fattori di SPID.
Anche nell'autenticazione, come in ogni attività umana, la sicurezza porta un po' di complicazioni.
Inserisco **username** e **password** sul computer, inserisco il **pin** di sblocco nell'App sul telefono, leggo il codice generato e lo inserisco sul computer. Sono tre-quattro passaggi, ma la sicurezza ha un piccolo costo e, comunque, è sempre più semplice e più veloce che trovare parcheggio davanti al municipio…

Chi controlla tutto? Che sicurezza c'è? I miei dati sono al sicuro?

I gestori dei servizi di autenticazione non possono usare i dati personali dell'utente né cederli a terzi senza autorizzazione da parte dell'utente. Tutti i log devono essere cancellati dopo un periodo prefissato.
Il sistema è composto da gestori pubblici e privati. Come ovvio, c'è la magistratura e poi, con funzioni specifiche, anche il Garante della Privacy e l'Agenzia per l'Italia Digitale. Le sanzioni in caso di comportamenti irregolari possono essere pesanti, arrivare fino a multe salatissime ed alla revoca dell'accreditamento, oltre ad altre sanzioni civili ed – eventualmente – penali.
Puoi leggere anche la sezione sotto: [Perché ci sono tanti fornitori di servizi di autenticazione? Perché anche privati?]

Perché ci sono tanti fornitori di servizi di autenticazione? Perché anche privati?

Questo fu un punto che inserii fin dalla mia proposta iniziale di un sistema di autenticazione con valore legale.

Una prima ragione riguarda la tenuta del sistema. Il modello di Internet è stato concepito proprio pensando all'assenza di un punto unico di governo della rete. La resilienza di Internet non è data dalla sua robustezza ma dalla sua anti-fragilità: ogni pezzo può essere vittima di un attacco ma il sistema nel suo complesso può continuare a funzionare. Dal punto di vista della resilienza, un sistema composto da più soggetti è più antifragile di uno centralizzato, in caso di un attacco.

Ma la mia motivazione principale fu un'altra. Proiettiamoci qualche anno o decennio nel futuro. Saranno sempre più i servizi dematerializzati, svolti online, che richiederanno identità certe. Dall'ottenimento di un finanziamento, all'accesso ad un concorso, alla difesa in un processo amministrativo, alla sottoscrizione di un referendum, ecc.

Supponiamo di concentrare il governo di tutte queste autorizzazioni in un solo punto. Chi lo controlla ha un potere immenso, esercitabile con grande velocità e – potenzialmente – opacità.

Per questa ragione la Costituzione della Repubblica Italiana, all'articolo 5, non modificabile, recita:

La Repubblica, una e indivisibile, riconosce e promuove le autonomie locali; attua nei servizi che dipendono dallo Stato il più ampio decentramento amministrativo; adegua i principi ed i metodi della sua legislazione alle esigenze dell'autonomia e del decentramento.

Questo articolo fu inserito in Costituzione perché emergevamo dalle lacerazioni della guerra e del ventennio fascista con la paura di creare condizioni che favorissero pulsioni autoritarie che si volevano evitare per il futuro.

Noi diamo per scontati tanti valori della vita democratica che scontati non sono.

Gli esempi abbondano, con tentativi (alcuni riusciti ed altri no) anche nella storia italiana, eppure li consideriamo devianze da una normalità.

In realtà è la democrazia ad essere una eccezione. La regola, purtroppo, sono sistemi autoritari.

Non dimentichiamo che per entrare in un sistema autoritario basta votare mentre non è altrettanto semplice uscirne.

La democrazia va tutelata costruendo nei momenti di luce le salvaguardie strutturali che ci tutelino nei momenti bui.

Il Prof. Lessig, costituzionalista americano di fama mondiale, giustamente ha osservato che "code is law", il codice informatico è una forma di legge, in quanto, al pari delle leggi, ci consente o meno di fare determinate cose. Come ad esempio quelle abilitate (o vietate) da un sistema di autenticazione.

Spesso identifichiamo "lo Stato" con il Governo. Ma non è così. Il Governo è solo uno dei poteri dello Stato. Montesquieu è considerato il padre dello Stato moderno con la tripartizione dei poteri (legislativo, esecutivo e giudiziario), con meccanismo di controlli e di bilanciamenti.

Sotto il controllo di quale potere avrebbe posto il codice informatico, il sistema di autenticazione? Sotto quello verticalmente integrato del ministro pro tempore degli interni e degli ordini impartiti ai suoi sottoposti o sotto il sistema giudiziario?
Un sistema di autenticazione online non è come una credenziale cartacea. La carta d'identità, una volta che viene emessa e consegnata alla persona, può essere usata ovunque senza che chi la rilascia abbia contezza se è stata usata per dimostrare la maggiore età entrando in un locale o per iscriversi ad un servizio di sostegno psicologico.
Una autenticazione online è permanentemente connessa consentendo potenzialmente di accumulare informazioni e, soprattutto, può essere inibita alla velocità della luce.
Un gestore privato di un servizio di autenticazione è sottoposto alla vigilanza del potere giudiziario, del Garante della Privacy e dell'Agenzia per l'Italia Digitale (AgID) che ne risponde in Europa, [come spiegato poco più in basso: "Come funziona in Europa"].
Un sistema di autenticazione condiviso consente di aumentare l'efficienza del sistema e certamente un sistema centralizzato potrebbe essere in linea teorica un po' più efficiente (costerebbe un pochino meno) e, se si trattasse di una azienda, quindi, probabilmente preferibile. L'estremo opposto precedente a SPID, ovvero in cui ciascuno costruiva e gestiva il proprio sistema di autenticazione, è certamente inefficiente e limitante.
Ma non bisogna dimenticare che lo Stato non è il Governo e non è nemmeno un'azienda. Va trovato un punto di equilibrio tra efficienza e salvaguardia del sistema democratico e di tutela dei diritti dei cittadini. Un sistema federato con gestori pubblici e privati, vigilati dalla magistratura, dal Garante della privacy e dall'AgID, in cui ciascun cittadino può ottenere credenziali da più fornitori è l'architettura che massimizza l'efficienza nel rispetto del dettato Costituzionale e nella tutela dei diritti dei cittadini, oggi e nel futuro.

Come si sostengono gli Identity provider? Vendono i nostri dati ?

No!.

Non possono svolgere alcun tipo di profilazione né tantomeno vendere i dati! [vedi sezione "Chi controlla tutto? Che sicurezza c'è? I miei dati sono al sicuro?"]
La legge prevede che gli enti pubblici che erogano servizi autenticati con SPID usino il sistema gratis. In genere gli Identity Provider privati sono soggetti che forniscono al mercato servizi che gestiscono la "fiducia digitale" come ad esempio posta elettronica certificata, archiviazione e conservazione dei dati, firma digitale, software di workflow certificato, ecc. Il fatto di essere gestori SPID gli dà un guadagno reputazionale che possono giocarsi sul mercato, non solo nazionale (alcuni di essi infatti operano in altri paesi, anche extraeuropei – una frontiera per servizi trusted "Made in Europe").
Inoltre, gestendo la app di autenticazione, hanno frequenti occasioni di contatto in più con i clienti, rimanendo loro "top of mind" per servizi di questo genere. Possono anche sviluppare

servizi integrati combinando elementi della loro offerta oggi a pagamento, mantenendo l'autenticazione gratuita. Gli sviluppi europei per i servizi fiduciari vanno verso una evoluzione della PEC e verso la creazione di "portafogli digitali" che in futuro potrebbero complementare la loro offerta di servizi, collegati all'identità SPID.
Teniamo presente che l'elemento più costoso è il riconoscimento iniziale che, se fatto remotamente, richiede un piccolo pagamento. Il costo variabile di una autenticazione è marginale.
Pensiamo a chi offre mutui, finanziamenti, ecc.: avere un dato certo grazie a del personale che verifica le identità, ad esempio presso un negozio di elettrodomestici, costa una decina di euro o più (che ricadono sul costo del finanziamento). Se divengono service provider autenticando gli utenti tramite SPID non usufruiscono del servizio gratuitamente: il costo base delle autenticazioni, è di 40c all'anno per utente.
Abbiamo infatti previsto nella legge che cittadini ed enti pubblici potessero usare i servizi gratuitamente e che gli altri fornitori di servizio pagassero. In particolare la legge prevede che le società che erogano servizi pubblici debbano adottare SPID entro una data che deve essere stabilita per decreto.
Pensiamo ad esempio al trasporto pubblico locale o al trasporto ferroviario o anche alle strutture sanitarie private (ospedali, laboratori, ecc.). Molti usano SMS per autenticare, un sistema meno sicuro, che ha un costo confrontabile se non maggiore. Oggi c'è una massa critica di utenti ed ormai c'è consuetudine all'uso di SPID, cose che potrebbero giustificare l'avvio dell'obbligo previsto dalla legge. Il beneficio sarebbe duplice: alimentare di risorse il sistema ed erogare un dato con una chiave di accesso comune. Ciò faciliterebbe l'implementazione di interoperabilità dei sistemi (per registrare anche i loro dati nel Fascicolo Sanitario Elettronico regionale e nel cassetto fiscale/dichiarazione precompilata). Discorso analogo può essere esteso a molti altri tipi di servizi.

Possiamo avere credenziali con più fornitori di servizi di autenticazione?

Sì.

È una caratteristica pensata by design sin dall'inizio, per aumentare il livello di privacy delle persone.

Puoi leggere anche la sezione precedente [Perché ci sono tanti fornitori di servizi di autenticazione? Perché anche privati?]

Non avrebbe senso un'interfaccia unica di accesso a tutti i servizi?

Certo, sarebbe bellissimo, se il mondo non fosse così complicato.

Ai vecchi di Internet come me questa idea ricorda romanticamente Yahoo.

A fine anni 90 Yahoo manteneva un elenco di tutti i siti web che apparivano online. Il modello "directory" andava per la maggiore. Ci mandavamo le mail per avvertirci "hai visto? C'è un nuovo servizio di previsioni meteo in Francia!"
Poi, con l'aumento esponenziale dei servizi web che nascevano, il modello directory non funzionava più e si impose il motore di ricerca.
In Italia ci sono oltre 13mila pubbliche amministrazioni ed ognuna di queste ha decine, centinaia di procedure che, nel tempo, verranno rese accessibili con SPID. Parliamo di una directory con centinaia di migliaia di servizi. (Inoltre ricordo che SPID può essere usato anche da gestori privati e lo sarà sempre di più).
È facile prevedere che il sistema prevalente per trovare il servizio cui vogliamo accedere sarà, come oggi, un motore di ricerca.
Ciò detto, c'è una pagina gestita da AgID che consente di trovare i servizi abilitati da SPID. [link]

Si possono avere due account SPID con uno stesso numero cellulare?

Il numero di telefono è un requisito che abbiamo inserito per avere un punto di contatto rapido con i cittadini e, oltretutto, facilita la registrazione e la generazione dei codici.
Quindi per ogni identity provider il numero di cellulare è legato ad una persona, e sarebbe meglio che la corrispondenza fosse univoca, anche per possibili ragioni di privacy. Per identity provider diversi, tuttavia, lo stesso cellulare potrebbe corrispondere a persone diverse (es. marito e moglie), se loro consapevolmente fanno registrazioni diverse con Identity Provider diversi con lo stesso numero di cellulare. In definitiva, se questa è una esigenza proprio non evitabile, basta usare due Identity provider diversi tra i 9 esistenti.

Non era più semplice usare Facebook o Google?

L'idea di proporre un sistema di autenticazione condiviso mi venne quando vidi molti anni fa qualche comune che iniziava ad erogare qualche servizio prendendo per buone le identità autodichiarate su Facebook.
Pensai che fosse una aberrazione, che non fosse possibile lasciare a una multinazionale l'autenticazione della nostra identità che deve essere garantita dallo Stato. L'identità è l'asset competitivo più estremo, non deve essere controllata da un monopolista non sottoposto alle leggi dello Stato. (Costituzione, art. 22: Nessuno può essere privato, per motivi politici, della capacità giuridica, della cittadinanza, del nome.)

Posso firmare con SPID? Cosa è una firma di un file?

La risposta breve è **sì.**
Molti lo hanno fatto di recente per i referendum.

Una firma di un file non è – come molti pensano – un autografo su un foglio, fotografato con il cellulare. Una firma siffatta ha un valore molto debole. In caso di contenzioso la sua validità, il fatto che corrisponda al presunto firmatario, deve essere valutata dal giudice. Di per sé ha il valore di una fotocopia e in mancanza dell'originale potrebbe non essere accettata. D'altro canto è molto facile prendere una foto di una firma e copia-incollarla su un documento. Insomma, va provato che sia vera.
Utilizzando SPID per provare la propria identità (nell'ambito di specifici sistemi di firma previsti dall'Agenzia per l'Italia Digitale) si può fare una firma elettronica più forte, che viene accettata come vera dal giudice in caso di contenzioso e che può essere disconosciuta solo denunciando per falso il suo autore. Insomma, va provato che sia falsa.
Una firma elettronica di questo tipo non è una immagine messa su una pagina di un file ma un insieme di bit ("quantità di sicurezza") incollata al file stesso. Questo insieme di bit è il risultato di operazioni crittografiche che matematicamente assicurano che quel file è integro e che non è stato manomesso.
Per firmare un documento che ci viene proposto da un fornitore un processo tipico potrebbe essere il seguente:

- ci facciamo riconoscere dal fornitore di servizio in modo giuridicamente certo usando SPID; in questo modo lui ci può proporre il documento da firmare essendo certo che non lo sta mostrando a terzi
- il fornitore ci propone il documento da firmare e, se accettiamo, gli appone una quantità di sicurezza e lo invia al nostro identity provider (quello che ci ha rilasciato le credenziali SPID)
- l'identity provider ci chiede di confermare la sottoscrizione chiedendoci una nuova verifica della nostra identità (non sia mai che il documento che gli è stato mandato sia diverso da quello che ci era stato mostrato!)
- Se confermiamo, autenticandoci, anche l'IDP appone una quantità di sicurezza e restituisce il documento a noi ed al fornitore e poi cancella il file (che così resta solo nella disponibilità nostra e del fornitore.

Attenzione, ci sono dei limiti a ciò che si può firmare. In generale, tutte le firme di atti tipicamente notarili…devono essere fatti davanti a un notaio.

Come funziona in Europa?

In Europa ci sono servizi analoghi previsti da un regolamento europeo chiamato **eIDAS** che prevede che le credenziali rilasciate in un paese siano accettate anche negli altri.
Per fare questo esiste una rete di nodi interoperabili che fungono da "ponte" tra Service provider e Identity provider di altri stati.

Una catena è robusta quanto il suo anello più debole. Dato che le credenziali rilasciate in un paese europeo sono valide negli altri, è importante che le regole del gioco ed il livello di fiducia sia analogo in tutta Europa.
Per questo ogni variazione delle regole di SPID va comunicato ai nostri partner europei e discusso con loro.

Lavoro in un'azienda che eroga servizi. Possiamo usare SPID?

Sì.
Se un privato qualunque vuole erogare un servizio essendo certo dell'interlocutore, può autenticare i suoi utenti con SPID con un costo modestissimo. Ci potrebbero essere dei rischi se ne venisse fatto un uso indiscriminato (ad esempio di accumulo di dati) per cui chi lo vuole usare deve accreditarsi presso l'Agenzia per l'Italia Digitale come descritto qui.
Prossimamente sarà inoltre possibile per i privati avvalersi di SPID utilizzando i servizi di aggregatori accreditati con l'AgID.

Dove posso vedere come sta andando SPID?

Nella sezione Avanzamento digitale del sito Agid [link]

Quando e come è nata l'idea di SPID?

Avevo scritto sul mio blog a marzo del 2012 un post con una prima riflessione di come migliorare l'autenticazione online dato i modestissimi risultati della carta di identità elettronica. Quello fu il momento di inizio delle riflessioni.
Il 6 gennaio 2013 ricevetti una telefonata di quelle che ti cambiano la vita.
Non essendomi mai occupato di politica prima, mi veniva chiesto di dare il mio contributo alla nascente lista civica dell'allora Presidente Monti. Avevo dei rapporti professionali in corso e non fu una decisione facile, ma alla fine accettai e venni eletto nelle elezioni del 24/25 febbraio 2013.
La settimana dopo le elezioni iniziai subito a proporre a colleghi di altri partiti e ad operatori del settore l'idea di un sistema di autenticazione, scollegato da un servizio specifico ma che fosse un servizio infrastrutturale a sé stante, federato e con valore legale. Il primo annuncio pubblico fu in questa intervista del 13 marzo.
Il 29 aprile, giorno della fiducia al Governo Letta, mentre ero in partenza per Roma feci un terribile incidente automobilistico che mi tenne tra la vita e la morte per una decina di giorni ed in ospedali e centri di riabilitazione vari per oltre 4 mesi. In quel periodo, con riunioni via telefono, skype e scambio di documenti via mail lavorammo alla definizione delle specifiche ed alla stesura della proposta di legge, sotto la guida esperta del grande Prof. Alessandro Osnaghi,

cui si deve la prima bozza di articolato, la grande collaborazione di Paolo Coppola con fondamentali giudizi e osservazioni sui casi d'uso pratici, il supporto legislativo di Eugenio Prosperetti (fondamentale nella prima stesura della Proposta di Legge).
In quel periodo (a fine giugno) il Presidente Letta nominò Francesco Caio commissario per l'attuazione dell'agenda digitale. Venne a trovarmi e discutemmo dell'importanza di un tale sistema che rientrò così, nelle sue tre priorità assieme ai progetti esistenti del polo dei pagamenti (oggi PagoPA) e della centralizzazione dell'anagrafe (ANPR).
Così da proposta di legge parlamentare – che non fu quindi nemmeno depositata – prese la corsia di sorpasso e divenne delega al Governo e successivo decreto della Presidenza (bozza), lavoro coordinato da Andrea Rigoni (cui si deve il nome SPID), con anche Giuseppe Caporello, Massimiliano Pianciamore, Annapia Sassano (grande concretezza e importanti i casi di vita vissuta), Stefano Arbia (che ne ha poi seguito gli sviluppi in Italia e in Europa) e di altri che certamente dimentico (mi scuso…).
Nel 2016 fu approvata la riforma del Codice dell'Amministrazione digitale cui avevamo lavorato per molti mesi con Paolo Coppola, Elio Gullo (del Ministero della Funzione Pubblica) e con il contributo di Sergio Boccadutri e degli avv. Eugenio Prosperetti e Guido Scorza (e, occasionalmente, di varie altre persone). In quella occasione introducemmo una innovazione che non era prevista nel regolamento europeo (eIDAS) ma nemmeno escluso: la possibilità di fare una "firma digitale" con SPID. Questa innovazione, a quanto so unica in Europa (almeno all'epoca), consente di usare le identità SPID per un vasto numero di usi con valore legale, ben oltre l'autenticazione.
Nel 2017 Paolo Coppola e Andrea Mazziotti avevano presentato due emendamenti (che avevamo sottoscritto con alcuni colleghi) per raccogliere le firme per le liste per le politiche, ma purtroppo furono bocciati. Riccardo Magi nel 2021 ne ha presentato uno per i referendum ed è stato approvato.

Del progetto di SPID cambieresti qualcosa?

In democrazia, le cose non vanno mai come decide una persona sola, ma tutte le scelte sono frutto di accordi e mediazioni tra varie parti interessate. Per questo non posso dire che cambierei cose frutto di mediazioni, ma solo cose che dipesero da me.
In quell'articolo del marzo 2013 in cui parlai di "identità digitale", tornando indietro forse userei termini diversi.
La parola "identità" in informatica ha una accezione ben precisa che non corrisponde alla idea che ne può avere un non informatico. Forse sarebbe più preciso autenticazione, identificazione, autorizzazione (o forse no, anche qui, giuridicamente, il significato di queste parole è diverso dall'accezione informatica).
Forse "gestione e verifica di credenziali".