

Spid e identità digitale

## Spid e identità digitale

Dr. Paolo Luppi - [pluppi@asol.it](mailto:pluppi@asol.it)

2 Febbraio 2017 - Sala Falck Fondazione Ambrosianum – Via delle Ore, 3 - Milano

## Identità digitale - definizione

Definizione di identità digitale: l'eID è l'insieme di attributi relativi ad una entità (persona fisica - persona giuridica).

Questi attributi possono essere informazioni personali. Tra di essi ve ne sono alcuni speciali denominati credenziali: sono utilizzati per potere accedere in modo sicuro a servizi.

Si ha un furto d'identità ogni volta che un'info individuale di PF o PG è ottenuta in modo fraudolento per compiere atti illeciti

## Indice

- Identità digitale e conseguenze dei furti
- Metodi di autenticazione forte: esempi pratici
- Innovazione digitale nella PA: dalla firma digitale allo Spid
- Spid: Pregi e limiti
- Consigli operativi per difendere l'identità digitale

## Furto di identità digitale - Metodologie di frode

Phishing o Ransomware

Siti internet

Skimming e sniffing

Spamming

Keylogging

Spoofing

## Furto di identità digitale – I danni

Attraverso finanziamenti illeciti si ottengono:  
80% casi finanziamenti finalizzati;  
10% per prestiti personali;  
7% carte di credito;  
3% altre frodi (fido conto/credito revolving)  
Profilo delle vittime – >50% tra 18 e 40 anni  
Tempi scoperta della frode – solo 33% in 6 mesi

## Furto di Identità digitale

Rischio perdite finanziarie ma anche  
reputazionali e riservatezza dati coperti da  
segreto professionale  
Perché si cade nella frode e perché non si  
prendono precauzioni ?

## Identità digitale - Privacy

Regolamento Privacy (UE) 27 aprile 2016  
Art. 5 – Principi applicabili trattamento dati  
Punto f) «integrità e riservatezza»  
«in maniera da garantire un'adeguata sicurezza  
Compresa la protezione mediante tecniche e  
organizzative adeguate, da trattamenti non  
autorizzati o illeciti e dalla perdita, distruzione o  
dal danno accidentali

## Identità digitale - Privacy

Novità Regolamento – Art. 87 in merito al  
trattamento del numero di identificazione  
nazionale  
Concetto di dato personale allargato in misura  
significativa (comprende anche ad esempio  
indirizzo Ip e i cookies).  
Potenziati diritti interessato – Tra i tanti diritto  
all'oblio, alla cancellazione e consenso esplicito.  
Obbligo della notifica violazione dati

## Furto identità digitali – Casi recenti

Yahoo - >500.000.000 dati

In Italia – Vulnerabilità della PA

Per alcuni esperti vi sono indicazioni di una carenza sistemica grave nella PA

Critiche del Garante Privacy in più occasioni in merito alla anagrafe tributaria

Archivio web: Have I been Pwned –verifica sicurezza account -  
<https://haveibeenpwned.com>

## Metodi autenticazione forte

Password e autenticazione

a) OAuth e Openid – sistema centralizzato di autenticazione  
Attraverso terze parti (es: Google per Dropbox – Spotify via Facebook)

b) Memorizzazione password a mezzo browser

c) Software gestione password (password manager) (es: 1password.com – keepass.info – lastpass.com)

d) Autenticazione a più fattori via due sistemi di riconoscimento separato (es: Bancomat con Pin e tessera – home banking con Password e token che genera chiavi numeriche temporanee)

e) Single Sign on (SSO) – unica autenticazione valida per più sw o risorse informatiche

## Innovazione nella PA: dalla CNS allo Spid

Utilità Single Sign On accesso alla PA

Presenza di vari sistemi di autenticazione (semplice password – Carta Nazionale dei Servizi – carta identità elettronica – Tessera sanitaria Carta Regionale dei Servizi)

SPID, Sistema pubblico di Identità Digitale, soluzione SSO federativo che permette di accedere a tutti (??) i servizi online della Pubblica Amministrazione con una unica identità Digitale (username e password) utilizzabile da computer, tablet e smartphone

## Spid – Sistema pubblico di identità digitale

Modulo\_di\_Richiesta

Se il documento non viene correttamente visualizzato nel box sottostante, è possibile visualizzare il pdf scaricandolo sul proprio computer. [Scanna PDF](#)



- Dichiaro di aver letto e compreso le previsioni contenute nella sezione relativa alla 'Richiesta di certificato OneShot' all'interno del documento soprariportato e di voler sottoscrivere digitalmente la stessa.
- Dichiaro di aver letto e compreso le previsioni contenute nella sezione relativa alla 'Richiesta del servizio InfoCert ID' all'interno del documento soprariportato e di voler sottoscrivere digitalmente la stessa.
- Dichiaro di approvare specificamente ai sensi degli artt. 1341 e 1342 del codice civile le disposizioni delle Condizioni Generali dei Servizi di Identità Digitale di seguito indicate: 1.2. (Licenza d'uso); 1.6. (Adeguamento, manutenzione, aggiornamento del Servizio); 1.6.1 (Cessazione e Sospensione del Servizio); 1.8. (Obblighi del Titolare); Art. 1.8.1 (Responsabilità amministrativa dipendente da reato); 1.9. (Obblighi di InfoCert); 1.10. (Uso illecito delle Identità Digitali); 1.11. (Accettazione Contratto / Clausola sospensiva); 1.12. (Durata del Contratto); 2.2. (Requisiti hardware e software); 2.3. (Connettività); 2.4. (Modificazioni in corso di erogazione); 2.5. (Corrispettivi); 3.2. (Identificativi ed accessi al sistema); 3.4. (Riservatezza e disciplina della proprietà intellettuale); 4.1. (Responsabilità del Titolare e dell'Intestatario della Fattura); 4.2. (Responsabilità di InfoCert e diritti del Titolare e dell'Intestatario della Fattura); 5.1. (Risoluzione); 6.4. (Foro competente).

## Spid – Sistema pubblico di identità digitale

### Dichiarazioni

#### Dichiarazioni

Il sottoscritto dichiara, nello specifico, di garantire

- al soggetto che effettua l'identificazione, per la richiesta delle credenziali di accesso, solamente dati, informazioni e documenti corretti, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci;
- la protezione e la conservazione con la massima accuratezza, al fine di proteggerne l'integrità, la segretezza e la riservatezza, della componente riservata delle credenziali di accesso, dei dispositivi sui quali sono trasmesse le OTP e delle OTP medesime nonché, se presenti, dei dispositivi crittografici contenenti le chiavi private associate a credenziali di livello 3;
- l'utilizzo delle credenziali di accesso per gli scopi specifici per cui esse sono rilasciate, ed, in particolare, per scopi di autenticazione informatica nello SPID, assumendo ogni eventuale responsabilità in caso di diverso utilizzo delle stesse;
- Di attenersi alle indicazioni fornite da InfoCert in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca dell'identità, alle cautele da adottare per la conservazione e protezione delle credenziali;
- l'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private;
- di non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi e regolamenti;
- l'adozione di ogni misura tecnica o organizzativa idonea a evitare danni a terzi;
- di non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalle consuetudini;
- di sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite e chiedere immediatamente all'IdP la sospensione delle credenziali;
- l'informazione tempestiva nei confronti dell'Identity Provider di ogni variazione degli attributi previamente comunicati, ai sensi dell'art. 8 del DPCM. Il Sottoscritto dichiara infine di essere consapevole che la violazione di uno degli obblighi di cui sopra nonché di uno degli obblighi previsti al paragrafo 3.2 del Manuale Operativo costituiscono inadempimento essenziale ai sensi dell'articolo 1456 c. c. e dà facoltà ad InfoCert di risolvere il contratto. La risoluzione opererà di diritto al semplice ricevimento di una comunicazione, inviata da InfoCert tramite raccomandata A.R. o posta elettronica certificata, contenente la contestazione dell'inadempimento e l'intendimento di avvalersi della risoluzione stessa.

Al sensi del D. L. n. 206/2005 «Codice del Consumo», InfoCert S.p.A. informa espressamente il richiedente che, prima della conclusione del contratto, ha diritto di revocare la presente richiesta attraverso apposita comunicazione da trasmettere, entro il termine di dieci giorni dall'inizio della richiesta, ad «InfoCert S.p.A., Piazza Luigi da Porto 3, 35131, Padova».

## Spid – Sistema pubblico di identità digitale

### Immagine accesso Spid



## Spid – Sistema pubblico di identità digitale

Un inizio non senza difficoltà

Vediamo le Faq principali pubblicate

**SPID è gratuito?**

Si, puoi richiedere gratuitamente le tue credenziali SPID a uno dei soggetti abilitati (Infocert, Poste, Sielte e TIM) Infocert e Poste, oltre alla modalità di erogazione gratuita, offrono anche una modalità di registrazione che invece è a pagamento.

## Spid – Sistema pubblico di identità digitale

**In che modo i gestori di identità (identity provider) verificano l'identità dei cittadini?**

L'utente può scegliere tra diverse modalità di riconoscimento offerte dai gestori d'identità, ad esempio:

- Identificazione a vista del soggetto richiedente
- Identificazione a vista da remoto
- Identificazione informatica tramite documenti digitali di identità (Esempio CIE/CNS)
- Identificazione informatica tramite firma elettronica qualificata o firma digitale.

## Spid – Sistema pubblico di identità digitale

### Come vengono trattati i dati personali?

Gli Identity Provider non possono utilizzare i dati personali dell'utente né cederli a terze parti senza autorizzazione da parte dell'utente stesso. Al momento della registrazione dovranno essere esplicitamente distinti i dati necessari all'ottenimento dell'identità digitale SPID dalle ulteriori informazioni - non obbligatorie - che il gestore di identità potrà eventualmente richiedere. L'Agenzia per l'Italia Digitale vigila sul rispetto delle norme in collaborazione con il Garante per la Privacy, sia per ciò che concerne l'attività degli identity provider, sia per quanto riguarda i servizi messi a disposizione da pubbliche amministrazioni e privati.

## Spid – Sistema pubblico di identità digitale

### Come vengono trattati i dati che fornisco per richiedere SPID?

I dati personali che comunicherai a Infocert, Poste, Sielte o Tim per richiedere SPID, non verranno utilizzati a scopo commerciale. Con SPID la tua privacy è totalmente garantita.

### Tutte le amministrazioni consentiranno l'accesso ai propri servizi tramite SPID?

Sì, l'adesione dell'intera pubblica amministrazione a SPID dovrà avvenire entro il 2017.

## Spid – Sistema pubblico di identità digitale

### Che differenze ci sono fra i tre livelli di sicurezza delle credenziali SPID?

- Il primo livello permette di accedere ai servizi online attraverso un nome utente e una password scelti dall'utente.
  - Il secondo livello – necessario per servizi che richiedono un grado di sicurezza maggiore - permette l'accesso attraverso un nome utente e una password scelti dall'utente, più la generazione di un codice temporaneo di accesso (one time password).
  - Il terzo livello, oltre al nome utente e la password, richiede un supporto fisico (es. smart card) per l'identificazione.
- Ad oggi sono disponibili solo identità SPID di primo e secondo livello.

## Spid – Sistema pubblico di identità digitale

### Qual è la differenza tra SPID e la Carta Nazionale dei Servizi?

I due strumenti hanno usi e scopi in parte diversi e in questa prima fase di implementazione del sistema SPID coesisteranno.

A differenza della Carta Nazionale dei Servizi - che non è completamente dematerializzata - per l'uso dell'identità SPID non è necessario alcun lettore di carte e può essere utilizzata in diverse modalità (da computer fisso o da mobile).

### I cittadini che già hanno strumenti di accesso ai servizi della PA (Carta Nazionale dei Servizi, registrazioni presso singoli siti, ...) potranno utilizzare ancora questi strumenti una volta preso SPID ?

Nella prima fase di avvio del sistema pubblico di identità digitale la necessità è quella di far coesistere il sistema di autenticazione tramite SPID con quelli già esistenti.

La progressiva implementazione del sistema da parte della pubblica amministrazione (che durerà 24 mesi) farà sì che tutti i servizi online siano accessibili tramite SPID.

## Consigli operativi per difendere l'identità digitale

a) Conservare le credenziali di autenticazione con sistemi robusti.



## Consigli operativi per difendere l'identità digitale

b) Non utilizzare per navigare con Spid o in banca lo smart phone in cui ho installato l'app di generazione delle credenziali.

c) Cancellare i dati raccolti dal pc/smart phone con gli appositi software (es: Ccleaner).

d) Effettuare pagamenti su internet con carte prepagate o virtuali o con metodi sicuri (es: Paypal)

## Consigli operativi per difendere l'identità digitale

e) Utilizzare account temporanei per iscrizioni su siti se vi è dubbio garanzia privacy (es: [www.10minutemail.com](http://www.10minutemail.com)).

f) Cambiare tutte le mail di default.

g) E soprattutto grande prudenza e attenzione quando si naviga e si gestisce posta elettronica

Grazie per l'attenzione

Paolo Luppi - [pluppi@luppi.it](mailto:pluppi@luppi.it)