Ordine degli Ingegneri della Provincia di Roma

GIORNATA MONDIALE DELLA SICUREZZA:

La Sicurezza nella pubblica amministrazione

La gestione dell'Identità Digitale e la sicurezza informatica

Ing. Paola Rocco

28 Aprile 2016

Indice degli argomenti:

- Cosa è SPID
- Cosa devono fare le PA e gli utenti finali
- L'architettura AAA
- Vantaggi e svantaggi

Cosa è lo SPID (1/2)

"**S**istema **P**ubblico dell'**I**dentità **D**igitale"

"Sistema pubblico dell'identità digitale" (Spid), con cui si può accedere a servizi pubblici e - in futuro- privati con un solo sistema di password.
Lo scorso 15 marzo il **Sistema Pubblico di Identità Digitale** (SPID) è diventato una realtà tangibile, con la possibilità per cittadini e imprese di farsi rilasciare, dai gestori accreditati presso AgID, le identità digitali per la fruizione di servizi pubblici e privati tramite un'unica e diffusa infrastruttura di identificazione.

Entro il 2018 tutte le PA dovranno integrarsi e si potrà accedere ai servizi online in soli 3 modi:

1. Carta nazionale dei servizi
2. Carta d'identità elttronica
3. Spid

Cosa è lo SPID (2/2)

Un nome utente e una password complessa, che il cittadino può ottenere in vari modi da un provider (quale Tim, Poste Italiane e Infocert).

- TIM bisogna andare su www.nuvolastore.it, registrarsi per ottenere un "TimId", ma bisogna avere almeno una di queste cose per riuscirci: la Carta Nazionale dei Servizi, la Firma digitale, la Carta di Identità Elettronica. Entro fine anno Tim abiliterà anche alcuni negozi per fornire l'identità di persona (a fronte di normali documenti di identità)
- Poste Italiane: registrandosi sul sito con la Carta Nazionale dei Servizi, la Carta d'identità elettronica, la firma digitale oppure come cliente di Poste Italiane (tramite strumenti di identificazione come lettore BancoPosta, numero di telefono certificato su carta Postepay o Libretto Smart, APP PosteID)oppure all'interno di 360 uffici.
- Infocert:sul sito https://identitadigitale.infocert.it per ottenere l'identità tramite riconoscimento via webcam (a 15 euro) oppure con Firma digitale, Carta Nazionale dei Servizi o Carta d'Identità elettronica. In alternativa possiamo andare in un ufficio Infocert di persona, per ora solo Roma, Milano o Padova

Cosa consiste l'identità digitale

L'identità SPID è 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.

Servizi attivi

spid
Sistema Pubblico
di Identità Digitale

Fonte AgID

Accesso ai servizi: Identity Provider e Services Provider ruoli e responsabilità

- **Nessuna banca dati centralizzata delle identità.** Per proteggere la privacy degli utenti, ogni IdP sarà responsabile dello svolgimento in modo sicuro delle attività connesse, mentre ogni service provider – pubblico o privato – avrà accesso solo ai dati di cui ha bisogno per erogare il servizio.

- Utilizzando **diversi IdP** il sistema è più sicuro e meno vulnerabile; non esiste un singolo elemento che possa interrompere il servizio e nessun servizio unico che disponga di tutti i dati in un unico luogo.

- 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.

- È protetto da un punto di vista civile **dalle norme che regolano SPID**, ma anche dal codice penale che in questo caso prevede la reclusione fino a tre anni (oltre ad una multa) per il gestore di identità (art. 640-quinquies del codice penale). Altre norme sono applicabili al gestore di identità in quanto agisce in qualità di gestore di servizio pubblico.

Fonte AgID

Accesso ai servizi: Identity Provider e Services Provider ruoli e responsabilità

- l'uso dell'identità SPID tale reato (**sostituzione di persona, frode informatica**, ecc.) sarebbe facilmente provabile. Il gestore dell'identità infatti deve mantenere traccia dei processi di autenticazione effettuati.

- In osservanza alle direttive del garante Privacy, **un SP può ottenere da un IDP o da un AA solo gli attributi necessari per la verifica delle policy di accesso al servizio richiesto** – comunicate agli utenti alla registrazione al servizio specifico e per le quali ha ricevuto esplicito assenso - e utilizzarli puntualmente solo a questo fine.

- l'interoperabilità del sistema SPID nel panorama tecnologico europeo. In questo quadro, SPID si basa sulle specifiche OASIS SAML v2.0 molto diffuse a livello europeo e adottate nel progetto sperimentale Stork (un progetto condiviso su larga scala da molti Paesi europei che mira a sviluppare un'infrastruttura comune per l'identità digitale, sia per le persone fisiche sia per quelle giuridiche).

Fonte AgID

Requisiti di sicurezza che deve rispettare il IdP (1/3)

1. Il gestore redige un piano per la sicurezza nel quale, al fine di descrivere l'attività di gestore di identità SPID, sono contenuti almeno i seguenti elementi inerenti alla attività di gestore di identità:
a) struttura generale, modalità operativa e struttura logistica;
b) descrizione dell'infrastruttura di sicurezza fisica;
c) allocazione dei servizi e degli uffici negli immobili;
d) descrizione delle funzioni del personale dipendente preposto alle attività necessarie all'esercizio e sua allocazione;
e) attribuzione delle responsabilità ai dipendenti del gestore;
f) algoritmi crittografici o altri sistemi utilizzati per garantire la sicurezza delle informazioni;
g) descrizione delle procedure utilizzate;
h) descrizione dei dispositivi installati;

Fonte AgID

Requisiti di sicurezza che deve rispettare il IdP (2/3)

i) descrizione dei flussi di dati;
l) procedura di gestione delle copie di sicurezza dei dati;
m) procedura di continuità operativa del servizio di autenticazione, revoca e sospensione;
n) analisi dei rischi;
o) descrizione delle contromisure;
p) descrizione delle verifiche e delle ispezioni;
q) procedura di gestione dei disastri;
r) procedura di gestione degli incidenti;
s) misure di sicurezza per la protezione delle credenziali degli utenti;

Fonte AgID

Requisiti di sicurezza che deve rispettare il IdP (3/3)

t) descrizione della conservazione delle credenziali fornite agli utenti e loro analisi al fine di sostenere la loro collocazione nel livello di sicurezza di cui al comma 1 dell'articolo 6 del DPCM 24 ottobre 2014 ritenuto appropriato. Al fine di distinguere nello scambio documentale con l'Agenzia le tipologie di credenziali fra loro, ad ogni tipologia è assegnato un riferimento univoco composto da aaaa_ss_mm dove, aaaa rappresenta l'anno in cui la tipologia di credenziali è presentata per la prima volta all'Agenzia per la valutazione prevista dal comma 2 del citato articolo del DPCM, ss è un numero sequenziale univoco nell'ambito di ogni singolo anno che individua la tipologia presentata nell'anno, mm è un numero sequenziale che afferisce alle eventuali modifiche successivamente presentate per la singola tipologia;
u) le idonee misure di sicurezza adottate, ai sensi dell'articolo 31 del Codice, rispetto ai rischi di accesso improprio, distruzione o perdita dei dati personali o della loro disponibilità e integrità, furto, uso abusivo, alterazione o usurpazione di identità, ripudio o disconoscimento di una transazione, trattamento non consentito o non conforme alle finalità della raccolta.

Fonte AgID

Conclusioni

Grazie per l'attenzione!

p.rocco@pec.ording.roma.it
paola.rocco@nttdata.com