Cassandra Crossing/ Difendiamo la SPID3

(395)— Un Sistema Pubblico di Identità Digitale sicuro non può fare a meno dei token hardware controllati dall'utente. Ma per…

Cassandra Crossing/ Difendiamo la SPID3

(395)— *Un Sistema Pubblico di Identità Digitale sicuro non può fare a meno dei token hardware controllati dall'utente. Ma per facilitare la vita ai pigroni e agli Identity Provider di restare ancorati alle insicure password si può cercare di snaturarlo*

27 febbraio 2017—Come i 24 lettori ricorderanno, avendo già subito in questa rubrica ben 5 esternazioni a riguardo, secondo Cassandra solo la SPID2 con token hardware e la SPID 3 con token crittografico avrebbero diritto di esistere. Perché? Perché la società dell'informazione richiede una cultura e una pratica della sicurezza; e un'infrastruttura nazionale collegata alla sicurezza informatica di tutti non può avere niente di meno che una sicurezza a due fattori (qualcosa che sai, più qualcosa che hai).La regolamentazione della SPID, analogamente a quella ormai collaudatissima della Firma Digitale, prevede che gli operatori che la implementeranno e che forniranno il servizio siano aziende, qualificate da AGID e operanti in regime di libero mercato e concorrenza.L'equilibrio tra interesse pubblico e interessi privati, quando funziona, è un'ottima cosa, ma per essere instaurato e mantenuto richiede una continua attenzione e una cura amorevole.

Infatti si potrebbe andreottianamente pensare che l'attuale assenza di un'offerta SPID2 con token OTP fisico e di SPID3 sia causata dal fatto che realizzarle in regime di gratuità non sia sostenibile a livello di business. Probabilmente è vero. Il risultato però è che il massimo di sicurezza che si può ottenere oggi come SPID è la SPID2 con token software.

Cassandra, il NIST e tanti altri (non in ordine di autorevolezza) hanno già dimostrato come questa soluzione non sia sufficientemente sicura. Uno smartphone con un'app è un oggetto troppo complesso per poter essere sicuro. Ma quando ci sarà la SPID3 i patiti del token hardware saranno soddisfatti? Non è detto, e spiegare il perché sarà un po' pesante. I 24 lettori sono avvertiti…

AGID ha creato nel 2015 un gruppo di lavoro allo scopo di definire uno standard UNINFO per i requisiti di sicurezza che un Identity Provider SPID deve soddisfare per essere accreditato.

Attualmente l'adeguatezza dell'Identity Provider è infatti lasciata alla discrezionalità della valutazione e degli audit di AGID. Questo documento che definirà lo standard, di cui si è discusso durante l'edizione XIX di e-privacy, è adesso in votazione nell'organo tecnico UNI/CT 510/GL 02 ed è intitolato *"E14.J1.G62.0 Sicurezza delle informazioni Verifica dei livelli di garanzia dell'autenticazione*

informatica Valutazione della conformità ai Livelli di garanzia 2, 3 e 4 della norma UNI CEI ISO/IEC 29115".

SPID3 corrisponde al livello di assurance 4 (LOA4) dell'ISO 29115, che *richiede* (ripetiamo "richiede") l'utilizzo di dispositivi *fisici* (ripetiamo "fisici") sotto il controllo dell'utente.

Lo standard in corso di valutazione non permette, per realizzare SPID3, l'utilizzo di due soluzioni che per l'Identity Provider sarebbero particolarmente facili ed economiche (qualcuno ha detto "appetibili"?) da implementare:- l'utilizzo di App "interamente software" da installare sullo smartphone dell'utente. Vi ricorda qualcosa?- l'utilizzo di dispositivi di firma remota come strumenti di autenticazione SPID. E qui potrebbe cascare l'asino!Parentesi: la firma digitale remota è un altro esempio di smaterializzazione del token, concepita solo per esigenze particolarissime come i sistemi informatici delle pubbliche amministrazioni, ma oggi venduta con successo ai privati pigri, che sono ben contenti di non doversi portare dietro la smartcard e di cavarsela con una password. Metà delle firme digitali attive in Italia sono ahimè diventate di questo tipo, perché si tratta un prodotto "conveniente" sia per i privati che per le aziende. Peccato che siano meno sicure; ed evviva la cultura e la pratica della sicurezza!Torniamo allo SPID3. In pratica con questa soluzione, i requisiti di SPID3 si applicherebbero al dispositivo remoto situato presso l'Identity Provider, e l'accesso dell'utente al dispositivo di autenticazione potrebbe anche avvenire (ma vedi un po'!) con una semplice password. E comunque non sarebbe "qualcosa che hai". Mamma mia!

Di conseguenza, alcuni soggetti stanno, legittimamente, premendo per rendere inefficace questa parte dello standard o per modificarla. Sono tra quelli che stanno votando il nuovo standard? Fatevi la domanda, datevi la risposta.

Speriamo che in questo caso sia possibile sapere chi sono, anche se il processo di votazione (che termina in questi giorni) non è pubblico. Il fatto che la questione sia in votazione renderebbe tracciabili i tentativi di modifica, ma non permetterebbe di impedirli.D'altra parte il processo prevede la possibilità che AGID alla fine possa non tenerne conto.Perciò niente profezie oggi. Limitiamoci a sperare bene!

Marco Calamari—@calamarim

Le profezie di Cassandra: @XingCassandra

Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

Originally published at punto-informatico.it.

By Marco A. L. Calamari on February 8, 2022.

Canonical link