

Informatica

Firma digitale tra grandi prospettive e false partenze

di Nicola Bortolotti

Potrebbe sembrare ad un tempo imbarazzante e frustrante riprendere a distanza di un anno il tema della firma digitale annunciandone le “grandi prospettive” quando - nel primo numero del 2002 de “I Servizi Funerari” - si titolava “Firma digitale alla stretta conclusiva”.

In realtà la stretta conclusiva ancora non c'è stata, malgrado la maturità delle tecnologie e delle leggi (anche se in corso di profonda revisione), ed è dunque a questo punto opportuno analizzare criticamente che cosa sia effettivamente successo nel corso di questi ultimi dodici mesi in modo da potere ragionevolmente prevedere quali novità contraddistinguono il futuro prossimo, fermo restando che per il futuro remoto la strada è già da tempo irreversibilmente delineata e non potrà non vedere il prepotente affermarsi della firma realmente sicura.

Procedura provvisoria dopo la proroga

L'emblema della situazione è ben riassunto dalla storia del registro (informatico) delle imprese, la prima iniziativa di diffusione capillare e su scala geografica nel nostro paese della firma digitale.

Come si ricorderà la legge finanziaria 2002 (art. 3 comma 13 della legge 28 Dicembre 2001, n. 448) concesse una più che opportuna proroga di un anno all'obbligo della presentazione delle domande e denunce firmate digitalmente all'ufficio del registro delle imprese (per via telematica o su supporto informatico). Tale imposizione dell'utilizzo della “digital signature” sancita dall'art. 31, comma 2, della legge 24 novembre 2000, n. 340, all'epoca apparve prematura, vista la scarsa e non omogenea diffusione delle necessarie “smart card” fra le imprese e i commercialisti nonché dei software necessari per la firma vera e propria.

L'obbligo è scattato lo scorso 9 dicembre ma, ancora una volta, è stato preceduto da misure prudenziali, questa volta una circolare del Ministero delle Attività Produttive, la n. 3553/C del 29 Novembre 2002, che concede una finestra di sette mesi (ossia sino al 9 Luglio 2003) di regime transitorio durante il quale sarà consentita la presentazione su supporto informatico “anche in assenza di firma digitale, purché il floppy disk contenente il modulo informatico sia accompagnato da una distinta sulla quale siano apposte le firme richieste e siano contemporaneamente presentati gli atti previsti in formato cartaceo”. “Contestualmente alla presentazione della prima domanda (...) con la predetta procedura provvisoria, un rappresentante legale dell'impresa presenta richiesta per il rilascio gratuito del certificato elettronico di sottoscrizione e della smart card (...). Sono ovviamente ammessi dispositivi di firma digitale rilasciati da altri distributori autorizzati”.

La circolare 3553/C

Nella importante circolare (che stranamente e colpevolmente non viene citata nelle pagine web di Infocamere dedicate alla firma digitale raggiungibili all'indirizzo www.card.infocamere.it - che invece si limitano unicamente a porre in evidenza con grande risalto l'entrata in vigore dell'art. 31 della legge 340/2000) - correttamente richiamata, invece, nei siti e nelle comunicazioni delle singole Camere di Commercio - si pone l'accento su alcuni fatti importanti: “Tali iniziative [non solo le leggi citate ma anche altre misure come i decreti 21 marzo 2001 e 19 marzo 2002 per la sperimentazione del deposito per via telematica del bilancio, il decreto 12 novembre 2001 per la presentazione per via telematica degli atti di conversione del capitale sociale in Euro] hanno favorito il diffondersi dell'uso della firma

digitale tra gli utenti del registro delle imprese, ma il numero di dispositivi di firma rilasciati (circa 200.000) dovrà ancora essere incrementato per garantire la piena funzionalità degli uffici del registro delle imprese a seguito dell'introduzione delle nuove procedure informatiche".

E ancora: "Assistiamo al contempo all'evolversi del quadro normativo di riferimento: (...) al Dipartimento dell'innovazione e le tecnologie è in corso l'adozione del regolamento per il coordinamento tra il T.U. in materia di documentazione amministrativa approvato con il D.P.R. 28 dicembre 2000, n. 445 con le disposizioni contenute nel decreto legislativo n. 10 del 2002 di attuazione della direttiva 1999/93/CE per le firme elettroniche"; si tratta - in realtà - di un sofferto e costante sforzo normativo e di armonizzazione non solo italiano ma europeo, sia a livello centrale che dei singoli paesi membri.

È dunque bene soffermarsi sul paradigma della situazione fornito dalla circolare 3553/C.

Cosa decreta il successo di una tecnologia?

La domanda che può sorgere spontanea - dopo anni e anni di "false partenze" effettive e apparenti per la firma digitale - di fronte alla locuzione "evoluzione del quadro normativo", è innanzitutto questa: si tratta davvero di una tecnologia realmente sicura se ha bisogno di tali e tanti "aggiustamenti" ed "evoluzioni" addirittura prima del suo utilizzo su vasta scala?

La risposta è inequivocabilmente affermativa. I sistemi di crittografia a chiave pubblica (sui quali si basa la "digital signature", per avere un'idea dei quali si rimanda - fra l'altro - al citato numero 1-2002 de "I Servizi Funerari") sono una tecnologia assolutamente matura e impenetrabile, ampiamente collaudata e utilizzata, che si fonda su robuste fondamenta teoriche. Si tratta anzi di uno dei mirabili esempi che dimostrano come concetti in apparenza astratti e privi di utilità pratica della matematica (lo studio dei numeri primi e l'aritmetica modulare) e della logica (lo studio degli algoritmi e della loro complessità computazionale) possano trovare applicazione concreta e strategica dopo un percorso culturale di millenni.

Eppure, nel campo della tecnologia, non sempre la moneta buona scaccia quella cattiva; non sempre, non subito e non in ogni campo le creazioni geniali riescono ad avere successo.

A volte questo accade a causa dell'eccessivo anticipo sui tempi di un'idea rispetto alle tecniche in grado di concretizzarla: si pensi, ad esempio, alla sorprendente intuizione che la splendida e leggendaria

attrice Hedy Lamarr e il musicista d'avanguardia George Antheil concretizzarono in un pregevole brevetto del 1941, addirittura l'avanzatissimo sistema di modulazione ad espansione di spettro detto "Frequency Hopping" al quale - rimasto nel cassetto per quasi mezzo secolo - negli ultimi quindici anni sono stati dedicati centinaia di articoli delle IEEE transactions e che rappresenta uno dei cardini delle tecniche ECCM militari e delle Wireless LAN.

Altre volte questo succede per motivi - per così dire - "sociali".

Quest'ultimo è il caso della firma digitale, per varie ragioni che si elencheranno senza pretesa di eshaustività.

L'organizzazione del lavoro

L'adozione della firma digitale comporta necessariamente una profonda modifica dell'organizzazione del lavoro, a vari livelli e in maniera non sempre compatibile con le procedure ormai largamente acquisite dalla pubblica e privata amministrazione e burocrazia. Inevitabile che sorgano e sorgeranno forti resistenze all'introduzione delle nuove tecnologie, specie considerando il fatto che - soprattutto inizialmente - esse comporteranno un aggravio di tempi ed oneri di lavoro in alcuni settori nonché l'impossibilità di ricorrere a quelle forme di "disinvolve flessibilità", talora al limite del lecito ma "salvapratica" o "salvacontenzioso", alle quali si può essere affezionati e che - talora - sono l'unica ancora di salvezza nei confronti di rigidità operative come, ad esempio, il prevedere "buchi" temporali nel protocollo o l'apporre (beninteso autorizzati) "firme" per altri funzionari.

Si potrà - invece - spesso assistere ad una complicazione delle procedure anziché alla loro semplificazione, ad un aumento iniziale dei tempi anziché ad una loro riduzione, con conseguente delusione e irritazione da parte dell'utenza.

Questo anche a causa dell'attuale mancanza di software e modalità operative per la firma digitale che siano realmente facili ed immediate da utilizzare, che sappiano dunque imporsi sul mercato come prodotto di riferimento - con tutti i pro e i contro connessi - un po' come è accaduto nel mondo dell'Office Automation con l'avvento di Microsoft Office.

In realtà esistono già applicazioni dell'algoritmo di crittografia a chiave pubblica RSA che hanno "sfondato" e che sono quotidianamente utilizzate da milioni di persone: si pensi, ad esempio, a quando si compie una transazione "sicura" su Internet (in

qualsiasi ambito, sia esso bancario o amministrativo).

Dietro quel prefisso che da "http://" diventa "https://" c'è infatti il protocollo SSL che si basa proprio sulla firma digitale. Questo è un esempio di ciò che è gradito all'utente: una transazione sicura che non comporta nessun aggravio operativo. Questo è dunque quanto dovrebbe auspicabilmente diventare anche la firma digitale dei documenti, un qualcosa di facilissimo, di immediato per l'utente medio. Ma siamo purtroppo ancora assai lontani da questo obiettivo.

Il protocollo informatico

In questo quadro che vede forti difficoltà e dunque giustificabili resistenze (anche da parte dei privati) all'applicazione di una tecnologia matura, si situa dunque l'azione dei governi sulla Pubblica Amministrazione. Se la passata legislatura aveva avviato dal 1997 una possente opera di razionalizzazione e informatizzazione della P.A. (con esiti alterni, tanto che ancora oggi alcuni uffici si ostinano a richiedere certificati in luogo di autocertificazioni, giocando sulla mancanza di tempo e convenienza nell'aprire un contenzioso), l'attuale si trova l'arduo compito di completare la difficile opera sui vari fronti, ivi compreso quello della Carta d'Identità Elettronica. È dunque assai significativo l'impulso recentemente dato di concerto dai ministri Stanca (Innovazione e Tecnologia) e Mazzella (Funzione Pubblica) col comunicato stampa dello scorso 6 Dicembre nel quale si annuncia l'emanazione della direttiva "sulla 'Trasparenza dell'azione amministrativa e la gestione dei flussi documentali', ovvero il cosiddetto protocollo informatico", direttiva in corso di registrazione.

La direttiva

In particolare "dal primo gennaio 2004 la gestione e l'archiviazione di tutti i documenti della P.A. avverrà in via elettronica: questo consentirà di trasformare le pratiche presentate agli uffici pubblici in documenti digitali, permettendo la trasmissione e la gestione interna della pratica per via telematica ed eliminando il trasferimento fisico del fascicolo cartaceo". "La Direttiva (...) ha lo scopo di promuovere l'adozione del protocollo informatico in tutte le amministrazioni centrali e gli Enti pubblici non economici, favorendo così l'utilizzo esteso di documenti informatici e l'erogazione di servizi in rete a cittadini e imprese. Inoltre, in accordo con il

'Piano nazionale di e-Government', la Direttiva intende assicurare il più rapido e proficuo utilizzo della firma elettronica nello scambio di documenti e atti tra le amministrazioni".

Non solo: "grazie al protocollo informatico sarà possibile migliorare l'efficienza interna degli uffici attraverso l'eliminazione dei registri cartacei e la razionalizzazione dei flussi documentali. In questo modo anche cittadini e imprese - collegandosi in rete ai siti della Pubblica Amministrazione - avranno la possibilità di verificare lo stato delle pratiche".

La direttiva prevede in particolare l'istituzione di un Centro di competenza per il progetto protocollo informatico e trasparenza amministrativa che - raggiungibile all'indirizzo EMail cc@protocollo.gov.it - costituirà l'unico punto di riferimento per il progetto svolgendo funzioni di indirizzo e coordinamento e promuovendo l'attuazione della direttiva.

Allo scopo è stato anche predisposto un apposito sito raggiungibile all'indirizzo Internet protocollo.aipa.it che comincia già ad addensarsi di contenuti ed offre anche un forum di discussione riservato e una serie di preziose FAQ (Frequently Asked Questions), ossia risposte già pronte alle più comuni domande concernenti gli aspetti generali del protocollo informatico, gli aspetti organizzativi, l'archiviazione ottica, la firma digitale, la classificazione e fascicolazione.

Per avere un'idea dell'ampiezza del progetto - che ovviamente ha una parte assai importante nella formazione dei dipendenti e funzionari della P.A. con interventi mirati che hanno preso il via nel maggio scorso - basti ricordare che le amministrazioni che dovranno approntare il Protocollo Informatico - secondo il nuovo schema delle regole tecniche contenuto nel DPCM 31-10-2000 - sono tutte quelle definite dal DL 29/93, ossia: Amministrazioni Centrali, Enti locali, comunità, consorzi ed associazioni, Enti del S.S.N., Enti pubblici non economici, Istituti scolastici, Istituzioni universitarie.

Ovvio anche l'esigenza di provvedere - ove necessario - all'adeguamento di hardware e software usufruendo preferibilmente delle offerte Consip reperibili all'indirizzo www.acquistinretepa.it.

Dalle code al click

La via del protocollo informatico passa anche per un'attività di censimento e integrazione di quanto è già stato attivato dalle singole amministrazioni ma - non ultimo - anche per l'informare gli utenti della disponibilità di servizi on-line.

In questa ottica è stato realizzato nel maggio scorso l'opuscolo "Dalle code al click", a cura del Ministero per l'Innovazione Tecnologica (scaricabile all'URL

www.innovazione.gov.it/ita/news/allegati/MIT_Opuscolo.pdf) e vengono costantemente aggiornati i link accessibili attraverso il portale istituzionale www.italia.gov.it.

Sperimentazioni e progetti pilota

Per convincersi ancor di più delle "grandi prospettive" della firma digitale è sufficiente notare come le "false partenze" non abbiano minimamente raffreddato gli entusiasmi. Per citare solo due esempi: nel febbraio scorso il comune di Torino ha avviato una sperimentazione che è culminata in ottobre con l'ufficializzazione del progetto "Forniture Online", ossia della gestione in linea di gare pubbliche anche per forniture oltre i 200 mila euro.

Dovrebbe inoltre partire nel prossimo anno in alcune sedi la sperimentazione del cosiddetto "Processo Telematico" con la prospettiva di entrare a regime nel 2004. E intanto si moltiplicano i corsi di formazione e aggiornamento come ad esempio quello dal titolo "La firma digitale e il processo telematico" che avrà luogo a Reggio Calabria il prossimo 7 e 8 Febbraio (per informazioni www.posytronacademy.it).

L'importanza dell'utilizzo consapevole della firma digitale

Fra tanti fermenti e iniziative il 2002 verrà anche ricordato come l'anno delle polemiche e dei dubbi circa l'attendibilità della firma digitale.

Tutto è nato - in realtà - da un sostanziale equivoco che ha reso tuttavia evidente come un'adeguata formazione degli operatori e degli utenti sia assolu-

tamente irrinunciabile, anche a costo di uno slittamento dei tempi previsti.

La questione si può sintetizzare in breve: era stato fatto notare che un documento Word, pur se firmato digitalmente e riconosciuto come valido, poteva condurre alla stampa di informazioni diverse.

La cosa non deve sorprendere. La firma digitale si può infatti apporre a qualsiasi file, sia esso un documento o un programma. Ciò che viene garantita è l'integrità del file, non di ciò che scaturisce dalla stampa. Se - per fare un esempio - si firma digitalmente un programma che stampa l'attuale data e ora, una volta verificatane la firma si può essere certi che il programma sarà integro e farà ciò per cui è stato generato, ossia stampare data e ora (che cambiano costantemente).

Lo stesso discorso si può fare per un file Word, che può contenere sia informazioni statiche (ad esempio un testo), sia informazioni dinamiche (campi). A ciò si aggiunga il fatto che i word processors tipicamente reimpaginano dinamicamente il documento a seconda della stampante prescelta.

La firma apposta ad un file "doc", in sostanza, garantisce l'integrità del file Word in sé, ma certo non la "fedeltà" di ciò che viene stampato.

Dunque, nel caso di documenti aventi valore legale, ciò che si dovrà firmare non sarà mai il file Word (che può contenere elementi dinamici e che dunque non dà alcuna garanzia sul cosa e sul come verrà stampato) bensì un "qualcos'altro", un particolare file che si abbia la garanzia che verrà stampato "così com'è", ossia così come l'ha inteso e formattato l'estensore e firmatario.

Un formato di file "di stampa" che rispetta questi requisiti (a patto che si scelgano opportuni "fonts") e ha il grande pregio della portabilità (ossia di potere essere utilizzato su macchine con architetture differenti) è il cosiddetto PDF (Portable Document Format di Adobe), non a caso la tipologia di file prescelta da Infocamere per il suo programma di firma digitale.