# Le ragioni dei certificatori accreditati

di Giovanni Nasi – 20 novembre 2002

*(Relazione introduttiva del presidente di Assocertificatori al convegno Omat del 15 novembre 2002)*

**Un quadro introduttivo**

I certificatori sono prima di tutto imprese che cercano di trarre un beneficio economico dalla loro attività.
Questa affermazione può apparire una banalità, ma sento il bisogno di farla proprio perché finora non ha avuto un riscontro positivo.
Tutti i certificatori attivi in Italia, non fanno solo questa attività. In alcuni casi, anzi, si tratta di attività secondaria, se non marginale.
Per questo fatto e solo per questo fatto quasi tutti i certificatori iscritti nell'elenco tenuto dall'AIPA non sono ancora scomparsi dal mercato. Alcuni, per la verità, hanno mantenuto una posizione attendista, mentre i più attivi si sono dimostrati i certificatori iscritti all'Assocertificatori.

E' probabile che assisteremo a breve a nuovi casi di concentrazione, come già è avvenuto con la confluenza in ACTALIS delle attività di SIA e di SSB. Quindi in definitiva il numero dei certificatori "accreditati" è molto probabilmente destinato a ridursi.
Quali sono le cause di questo fenomeno?
La risposta a questa domanda ci riporta ai "contenuti" dell'attività dei certificatori e al contesto di mercato nel quale si sono trovati ad operare.

**I contenuti dell'attività dei certificatori**

Certificazione vuol dire dare certezza. Nel nostro caso parliamo di certezza sotto due diversi profili.

Un profilo di carattere giuridico: il certificatore garantisce l'identità del titolare del dispositivo di firma digitale. In altri termini, il certificatore, seguendo apposite procedure, identifica il soggetto al quale consegna il dispositivo ed emette un certificato digitale, contenente le generalità di tale soggetto.
Successivamente all'emissione, la responsabilità del certificatore consiste nel dare tempestivamente pubblicità alla revoca o alla sospensione del certificato. Se il titolare smarrisce la smart card e ne da comunicazione al certificatore, questi è tenuto a "pubblicare" immediatamente la sospensione. Nel caso in cui il ritardo sia fonte di danni per terzi, il certificatore ne risponde patrimonialmente.

Il secondo profilo che vede impegnato il certificatore è un profilo di carattere tecnico.
L'infrastruttura tecnologica necessaria è alquanto complessa e, per alcuni aspetti, inizialmente non reperibile presso i fornitori di mercato.
I requisiti tecnici di sicurezza previsti dalle norme emanate dal Governo sono, se vogliamo giustamente, molto stringenti. Le applicazioni sw e le apparecchiature hw devono aver passato il vaglio di certificazioni, al momento, ancora non emesse da nessun ente italiano.
Non nascondo, inoltre, che anche gli skill tecnici disponibili in Italia erano inizialmente quasi

inesistenti. Per cui i certificatori hanno dovuto affrontare una doppia difficoltà:
- formare le risorse umane in grado di approntare e gestire il servizio;
- reperire i sistemi aventi le certificazioni di sicurezza richieste e, molto spesso, stimolare i fornitori a dotarsi di queste certificazioni.

Credo di poter dire che i certificatori hanno svolto (e finora soprattutto) un'attività di divulgazione culturale a favore dell'impiego della firma digitale nelle transazioni telematiche.

Non solo. In molti casi il modo con il quale le P.A. hanno introdotto la firma digitale nelle loro procedure amministrative, si è rivelato molto oneroso per i certificatori. Sono state esperite gare per quantitativi talmente limitati, che i costi di partecipazione assorbono a priori anche le più rosee prospettive di margini.

In sintesi: la complessità dell'attività dei certificatori , unita alla "novità" dei sistemi impiegati ha reso impossibile fino ad ora per l'attività di certificazione di raggiungere il break even.
Non minore importanza ha avuto il ritardo – rispetto alle previsioni iniziali – con il quale si sta muovendo il mercato della firma digitale.
Le previsioni di partenza (siamo negli anni 1998-99) erano certamente influenzate dal clima di euforia nel quale si muovevano tutte le iniziative che avevano a che fare con Internet e con l'Information Technology.

Confessato questo "peccato originale", va detto però che, nel fare le previsioni di mercato, venivano considerati con priorità tre diversi segmenti:
- quello dei "pagamenti" sulla rete = cioè il trasferimento di fondi;
- quello dei "negozi giuridici" conclusi sulla rete;
- quello dell'e.government.

Finora la "firma digitale" a norma AIPA non è entrata in misura significativa nell'area dei pagamenti elettronici. Quella che sembrava una "logica adozione" dello strumento, anche per il valore probatorio riconosciuto al documento firmato digitalmente, non si è verificata.
Non ho gli elementi, né la competenza per tentare una spiegazione. Mi ostino a ritenere che la "logica adozione" prima o dopo si verificherà, forse una volta che siano state definitivamente superate le tante incertezze di carattere giuridico che hanno accompagnato il cammino della firma digitale.

Ma quello dei "pagamenti" non è l'unico segmento di mercato della firma digitale. C'è, subito dopo, quello dei "negozi giuridici" formati a distanza attraverso la rete.
La posta elettronica è sempre più utilizzata nel mondo degli affari. Richiesta di preventivi, presentazione di offerte, invio di ordini, accettazione di offerte: tutti atti che, se fatti attraverso Internet, possono essere attribuiti in modo non ripudiabile ad un soggetto solo se da lui firmati digitalmente.
E allora perché gli uomini di affari si affidano a mezzi giuridicamente molto meno consistenti? Perché la corrispondenza continua a girare su Internet senza nessuna forma di protezione?
Purtroppo la direttiva comunitaria recepita con il decreto legislativo 23 gennaio 2002 n.10, rischia di confondere le idee. Quale della gamma di firme elettroniche previste conviene utilizzare?
C'è il rischio che, a fronte della "forza unificante" del sistema creato dal D.P.R. 513/99 (valido sia per il "settore" pubblico che per quello privato), si vada ora verso una pluralità di "sistemi chiusi", cioè riconosciuti validi ciascuno in uno specifico ambito di attività.
Ma la firma digitale e la sua efficacia probatoria escono rafforzate dal decreto legislativo n. 10: "fa piena prova, fino a querela di falso, della provenienza da chi l’ha sottoscritto".
La norma fa proprio un orientamento autorevole della dottrina e prevalente della giurisdizione. Ed

"esalta" il ruolo e la responsabilità dei certificatori.
Mi sembra impossibile che il mercato (in questo caso fatto di uomini di business) non colga le opportunità offerte da questo strumento. Dal decreto legislativo n. 10, la "firma digitale", se avvalorata da un certificatore accreditato, esce come l'unica firma elettronica "sicuramente sicura", l'unica cioè che costituisca una prova inconfutabile della provenienza del documento sottoscritto.

Il terzo segmento di mercato della firma digitale è quello dell'e.government.
Non sto qui a illustrarvi i vantaggi dell'e.government.
Oggi abbiamo un Ministero con competenze ed esperienze professionali di altissimo livello in materia di tecnologie informatiche. Certamente il Ministro Stanca sa e vuole valorizzare le opportunità derivanti da questo nuovo modo di fare pubblica amministrazione.
L'e.government non si può fare senza investimenti e realizza economie di costi se adottato con soluzioni uniformi nei vari rami della P.A.. Se ogni ente la fa a modo suo (come risulta da uno studio di ASSOSOFTWARE di recente pubblicazione) gli investimenti aumentano, i benefici si riducono e gli utenti "si ribellano".

Ancora una volta: abbiamo uno standard, quello della firma digitale; ci sono imprese (i certificatori) pronte a offrire i servizi conformi allo standard. Perché molte Amministrazioni si ostinano a voler andare per conto loro?
Recentemente abbiamo inoltre saputo che SOGEI vuole distribuire gratuitamente a tutti i cittadini italiani una smart card in grado di contenere la firma digitale.
La "motivazione" è sempre la stessa: perché possa partire il piano dell'e.government occorre diffondere gratuitamente a tutti i cittadini i "sistemi abilitanti".
La verità è invece che bisogna assolutamente far decollare i servizi di e.government. Poi gli utenti (cittadini e imprese) sceglieranno liberamente a loro spese da quale certificatore (ce ne sono una quindicina) farsi rilasciare il dispositivo di firma.

Gli attuali certificatori sono in grado di soddisfare ampiamente la domanda di dispositivi. Ma se non ci sono servizi, la domanda non decolla e se si regalano le smart card, resteranno inutilizzate.

La nostra proposta è di stanziare le risorse necessarie per finanziare il progetto Sogei, sul fondo creato presso il Ministero dell'Innovazione e delle Tecnologie e con esso finanziare progetti di e.government delle pubbliche amministrazioni.