

PESCARA, 20 novembre 1999

Riccardo Ricciardi

ATTO NOTARILE INFORMATICO



In un'intervista a Repubblica del 6 novembre 1999 Franco Bassanini, sottosegretario alla Presidenza del Consiglio dei Ministri (la Firma Digitale italiana è nata in una delle Bassanini) ha asserito che "L'Italia per certi aspetti e' persino più avanzata degli USA. Per esempio, il riconoscimento pubblico della firma digitale, deciso dal governo Prodi, mi consente di comprare da Roma la villa di Cortina da un signore di Milano, facendo l'atto con un Notaio di Belluno, mentre tutti e tre restiamo a casa davanti al computer. E l'atto viene automaticamente trasferito – senza alcuna produzione di carta – al Pubblico registro e al Catasto."

Quest'asserzione, stante l'attuale normativa, è fuorviante, ma in un prossimo futuro potrebbero essere calzante.

E' vero infatti che le parti di una compravendita possono stipulare validamente il relativo contratto non muovendosi dalle rispettive città firmando il contratto informatico con la loro firma digitale: ma tale contratto non potrà essere trascritto perché privo della forma necessaria per la pubblicità immobiliare.

Stante l'attuale normativa, anche per le firme digitali e' prevista l'autentica notarile e, quindi, e' necessario che le parti si rechino, anche non contestualmente, da un notaio che a sua volta certificherà con la propria firma digitale che la parte ha firmato in sua presenza. Solo così il contratto di compravendita informatico autenticato nelle firme potrà essere trascritto.

Se poi le parti volessero l'atto pubblico, questo non potrebbe comunque essere stipulato telematicamente, poiché, a differenza delle scritture private autenticate, è richiesta la contestuale presenza di tutte le parti.

Riepilogando, con la normativa attuale utilizzando le varie combinazioni della firma digitale si possono ottenere i seguenti risultati:

Segretezza

Tizio perché il suo documento venga letto solo da Caio lo cifra con la sola chiave pubblica di quest'ultimo.

Caio potrà decifrare il documento con la sua chiave privata segreta ed asimmetrica.

Certezza di provenienza del documento da parte dell'autore

Tizio cifra il documento con la propria chiave privata.

Chiunque potrà decifrare il documento con la chiave pubblica asimmetrica di Tizio, sapendo così che il documento proviene da Tizio.

Segretezza del documento e certezza di provenienza da parte dell'autore

Tizio, per trasmettere a Caio un documento che solo Caio possa leggere e di cui Caio possa essere certo che proviene da Tizio, cifra il documento non solo con la propria chiave privata, ma anche con la chiave pubblica di Caio. In questo modo, il documento può essere decifrato solo da Caio, che deve però utilizzare non solo la propria chiave privata asimmetrica rispetto alla sua chiave pubblica apposta da Tizio, ma anche la chiave pubblica di Tizio asimmetrica rispetto alla chiave privata usata da Tizio.

Certezza di provenienza del documento da parte dell'autore e che il documento non è stato alterato

Tizio effettua un "hashing" (funzione unidirezionale, che a partire da un certo messaggio ricava un valore di lunghezza fissa, detto hash).

Tale funzione matematica genera, a partire da una generica sequenza di simboli binari, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.

Se il documento viene alterato, non si può più ottenere lo stesso hash.

In altri termini con la funzione di hash ("éntr e èsch" in dialetto campobassano) si riceve in entrata il documento informatico costituito da un enorme numero binario per ottenere in uscita un numero più piccolo, di dimensione costante, che è l'impronta del documento informatico.

Il documento informatico, quindi, è un documento cifrato, costituito da due files: il primo è il documento vero e proprio non cifrato, che può ovviamente essere letto da chiunque: il secondo è la firma digitale del documento che altro non è se non l'impronta ottenuta tramite la funzione di hash applicata al documento e cifrata con la chiave segreta dell'autore.

Se quindi Caio vuole controllare l'autenticità del documento di Tizio, applicherà al primo file, e cioè al documento presunto di Tizio, la funzione standardizzata di hash in modo da ricavarne l'impronta.

Indi, decifrerà il secondo file, ossia la firma digitale presunta di Tizio - cui è allegata obbligatoriamente, come da regolamento tecnico, il certificato corrispondente alla chiave pubblica da utilizzare per la verifica - apponendovi la chiave pubblica di Tizio stesso e ottenendo così la seconda impronta.

Le due impronte saranno perfettamente identiche, nel senso che saranno entrambe costituite da un identico numero di pochi byte, se l'autore del documento è anche l'autore della firma digitale; se le due impronte non coincideranno, anche di un solo bit, vuol dire che o il documento o la firma sono falsi.

Quindi su testi diversi non possono esistere due firme digitali uguali, perché ognuna contiene l'impronta del testo.

Infine, al documento può essere anche apposta la c.d. marca temporale, che è una firma digitale, apposta da un certificatore, che riporta l'indicazione del momento della firma, precisa e certificata e che non è da confondere con il certificato notarile.

Certezza di provenienza del documento da parte dell'autore, che il documento non è stato alterato e che è stato firmato dall'autore.

L'unico sistema relativamente certo per certificare che la firma digitale è stata apposta dall'autore del documento sembrerebbe, ancora una volta, l'intervento certificatorio di un terzo super partes: il notaio.

Il notaio assiste di persona alla concreta apposizione della firma, o meglio alla generazione della firma, da parte dell'autore sul documento informatico e ne certifica il fatto, previa identificazione del firmatario, con l'emissione di apposita certificazione a sua

volta firmata digitalmente. Per cui, a seguito della successiva verifica, si potrà avere la certezza dell'autore della firma e non soltanto del titolare della chiave.

Questo tipo di certificato viene definito notarile in contrapposizione al certificato d'identità che, invece, collega la chiave pubblica al soggetto,

Il certificato notarile viene quindi emesso dopo la relativa firma digitale e non può non essere che riferibile ad un singolo atto (mentre il certificato d'identità si riferisce ad un numero indefinito di futuri atti) e quindi non ha un termine di validità.

In effetti le differenze tra firma digitale autenticata e non autenticata non sono le stesse esistenti tra le corrispondenti firme su documento cartaceo, anche se norme del codice civile e del codice di procedura civile restano le stesse e cioè:

Art. 2702. Efficacia della scrittura privata.

La scrittura privata fa piena prova, fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.

Art. 2703. Sottoscrizione autenticata.

Si ha per riconosciuta la sottoscrizione autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.

L'autenticazione consiste nell'attestazione da parte del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il pubblico ufficiale deve previamente accertare la identità della persona che sottoscrive.

Art. 216 c.p.c. Istanza di verifica.

La parte che intende valersi della scrittura disconosciuta deve chiederne la verifica, proponendo i mezzi di prova che ritiene utili e producendo o indicando le scritture che possono servire di comparazione.

L'efficacia della scrittura privata informatica diviene in realtà diversa e superiore rispetto all'efficacia probatoria della scrittura privata cartacea come delineata nell'art. 2702 c.c. Infatti, "il giudizio di verifica di una firma digitale disconosciuta sarebbe concretamente un procedimento rapidissimo ed automatico, che potrebbe ugualmente e facilmente compiere chiunque, ottenendo riscontri oggettivi senza alcuna complicata indagine grafologica (Raimondo Zagami Valore giuridico della firma digitale e conclusione telematica del contratto) <http://www.interlex.com/docdigit/indice.htm> - docinf

La verifica di una firma digitale compiuta con una chiave pubblica certificata consente di ottenere un'identità soggettiva cui ricollegare la chiave stessa e dunque la firma. Si può così affermare con (relativa) certezza che la firma digitale verificata sia stata apposta con la chiave privata di titolarità del soggetto che risulta dal relativo certificato.

Inoltre le regole tecniche approvate con d.p.c.m. 8 febbraio 1999 stabiliscono che "il dispositivo di firma deve procedere all'identificazione del titolare" (art. 10 comma 4), negando così l'uso della chiave ad una persona diversa.

Quindi, in sostanza, la scrittura privata informatica, essendo sottoscritta con una firma digitale verificabile attraverso un valido certificato verrebbe ad avere la stessa efficacia di piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, come la firma cartacea autenticata.

Riconoscimento e disconoscimento/verifica sarebbero dunque, sostanzialmente irrilevanti e non più necessari. E, a differenza della tradizionale scrittura privata cartacea, si determinerebbe così sostanzialmente fin dall'inizio quell'inversione dell'onere della prova che pone a carico del titolare della firma l'onere di provarne la falsità - abuso della chiave privata.

D'altra parte, anche per la firma digitale autenticata occorrerebbe procedere ugualmente ad una verifica della firma digitale apposta dal pubblico ufficiale.

Conclusioni

La funzione del notaio non sarà quindi quella di semplice certificatore dell'identità delle parti (il cybernotary americano non ha il solo compito di certificare l'apposizione della firma digitale, ma anche di assicurare la legalità dei documenti destinati all'estero) ma di garante della legalità del documento informatico, sia esso privato o pubblico.

Legalità nel senso che il documento corrisponde alla volontà della parte, è conforme all'ordinamento giuridico ed è stato formato nel rispetto della procedura prevista.

Ai sensi dell'art. 16 del d.p.r. n. 513/1997, il notaio garantisce non solo la reale identità della parte che sottoscrive con firma digitale utilizzando la chiave privata ma indaga la volontà del sottoscrittore, realizzando la c.d. funzione di adeguamento; ed, infine, esegue il controllo di legalità e di conformità all'ordinamento giuridico dell'atto autenticato.

E tale funzione potrebbe già da ora (e lo potrà sempre più) essere svolta anche a distanza: da un notaio innanzi al quale le parti siano virtualmente presenti.

Secondo il codice deontologico l'"atto pubblico" costituisce la forma primaria e ordinaria di "atto notarile", che il notaio deve generalmente utilizzare nella presunzione che ad esso le parti facciano riferimento quando ne richiedono l'intervento, se non risulti una loro diversa volontà e salvo la particolare struttura dell'atto.

Ma nell'era informatica le funzioni riconosciute all'atto pubblico, presunte e reali (vedi per tutti Mariconda Gennaro in "Riv. not.", 1987, fasc. 2 (aprile), pt. 1, pag. 244-262) potranno sussistere solo equiparando la presenza virtuale delle parti alla loro presenza fisica e per fare ciò basterebbero queste semplici modifiche normative:

L. 16.02.1913 N.89 ART.47

ORDINAMENTO DEL NOTARIATO E DEGLI ARCHIVI NOTARILI

TITOLO III

Degli atti notarili

Capo I - Della forma degli atti notarili

47. L'atto notarile non può essere ricevuto dal notaio se non in presenza **anche virtuale** delle parti.

Spetta al notaio soltanto d'indagare la volontà delle parti e dirigere personalmente la compilazione integrale dell'atto.

CC 16.03.1942 N.262 ART.2699

ATTO PUBBLICO

1. L'atto pubblico è il documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato.

CC 16.03.1942 N.262 ART.2700

EFFICACIA DELL'ATTO PUBBLICO

1. L'atto pubblico fa piena prova, fino a querela di falso, della provenienza del documento dal pubblico ufficiale che lo ha formato, nonché delle dichiarazioni delle parti e degli altri fatti che il pubblico ufficiale attesta avvenuti in sua presenza **anche virtuale** o da lui compiuti.

In un prossimo futuro, quindi, l'atto notarile informatico potrebbe essere stipulato da un notaio alla presenza virtuale delle parti, previa loro identificazione biometrica, e firmato da tutti con firma digitale.

E in un lontano futuro, risolti i modelli matematici di strutturazione del cervello umano appena iniziati, potranno anche essere smentite le scettiche affermazioni che il computernotaio (una sola parola: non è un errore di digitazione) non vedrà mai la luce (o meglio non sentirà mai l'energia elettrica) perché incapace di colloquiare.