Firme elettroniche a valore legale internazionale: un nuovo approccio per migliorare l'interoperabilità (*)

Sommario: 1. Le firme elettroniche nel regime di cui alla direttiva europea del 1999; 2. Notai di tipo latino (*Civil Law Notaries*) e firme elettroniche; 3. Questioni strategiche in tema di verifica delle firme; 3.1 Molteplicità dei formati; 3.2 Differenze nei certificati di firma; 3.3 Marcature temporali; 3.4 Analisi dei risultati; 4. Possibili soluzioni; 4.1 Standards più dettagliati; 4.2 Applicazioni locali; 4.3 Un approccio alternativo: la piattaforma di verifica online; 4.3.1 Premesse; 4.3.2 Obiettivi del progetto; 4.4 Attuale stato d'avanzamento del progetto; 5. Conclusioni: uno sguardo al futuro

1. Le firme elettroniche nel regime di cui alla direttiva europea del 1999

La disciplina giuridica delle firme digitali in Europa è basata sulla Direttiva93/1999 (1), che detta la seguente nozione di "firma elettronica": *dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione*.

La Direttiva definisce altresì la "firma elettronica avanzata"; si tratta di una firma elettronica che soddisfi i seguenti requisiti:

(a) *essere connessa in maniera unica al firmatario;*

(b) *essere idonea ad identificare il firmatario;*

(c) *essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;*

(d) *essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.*

L'approccio della Direttiva si sviluppa su due fronti.

In primo luogo, si richiede agli Stati membri di provvedere affinché *una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è:*

- *in forma elettronica, o*
- *non basata su un certificato qualificato (2), o*
- *non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato (3), ovvero*
- *non creata da un dispositivo per la creazione di una firma sicura (4).*

In buona sostanza, ciò vuol dire che ogni firma elettronica, indipendentemente dalla sua intrinseca affidabilità (5), possiede un qualche grado di giuridica rilevanza in ogni Paese dell'Unione.

In secondo luogo, la Direttiva impone che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura:

a) posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei; e

b) siano ammesse come prova in giudizio.

L'attuazione della Direttiva nei vari Paesi Europei ha introdotto un'ampia varietà di sfumature nazionali, che non interessano però la nostra analisi [(6)].

2. Notai di tipo latino (*Civil Law Notaries*) e firme elettroniche

I notai di tipo latino sono stati tra i primi ad abbracciare le nuove tecnologie un po' ovunque in Europa. La ragione è semplice; con alcune differenze tra Paese e Paese, i notai latini [(7)], nella maggior parte dell'Europa continentale, sono una sorta di "sportello unico" [(8)] per i trasferimenti immobiliari e la costituzione di società. Le formalità successive sono eseguite dai notai sotto la loro responsabilità. L'acquirente di un immobile, per esempio, firma il contratto dinanzi al notaio, che si occupa di riscuotere le imposte ed eseguire le formalità e tutti i pagamenti dovuti. Nel far ciò, i notai generano una considerevole mole di dati che vengono introdotti in svariati Pubblici Registri; il sistema così garantisce la costante disponibilità di dati sempre affidabili, assicurando minor contenzioso e minori esigenze assicurative. La trasmissione dei dati in forma elettronica è una soluzione sempre più utilizzata e che presenta ovvi vantaggi; in questo contesto, le firme elettroniche rappresentano uno strumento utile se non indispensabile [(9)].

Se il trasferimento di dati su larga scala è quella che suol definirsi la *killer app* [(10)], i documenti notarili in forma digitale sono utili anche in altri campi. In Francia, si possono stipulare atti online anche se le parti sono in città diverse, purché sia disponibile un collegamento in videoconferenza ed un notaio sia presente in ciascuna località: l'atto sarà elettronicamente firmato sia dalle parti che dal notaio. Si possono inviare procure in tempo reale, e questo appare molto interessante in un'ottica internazionale: è anzi curioso che oggi si ricorra alla Rete per inviare documenti ad Uffici pubblici che magari distano poche centinaia di metri dallo studio del notaio, mentre i documenti diretti al di là degli oceani debbono necessariamente essere su carta. I notai europei certificano d'abitudine i poteri dei rappresentanti delle società commerciali: certificazioni elettroniche potrebbero essere disponibili istantaneamente ed ovunque, più affidabili ancora del loro equivalente cartaceo grazie alla firma digitale.

I notai e le loro organizzazioni hanno tempestivamente [(11)] visto nella firma digitale uno strumento per incrementare l'affidabilità del documento elettronico, portandola ad un livello paragonabile a quello dei documenti cartacei. Sono stati compiuti importanti investimenti infrastrutturali; smart cards ed altri dispositivi per la firma sicura sono diventati una presenza abituale negli studi notarili europei [(12)]. In linea con le tradizioni della professione, le organizzazioni notarili europee hanno prescelto la tecnologia più affidabile, quella che nel gergo

dell'Euroburocrazia si chiama *firma elettronica avanzata basata su un certificato qualificato*, detta anche *firma digitale* [(13)]: la tecnologia di firma basata sulla crittografia simmetrica ed un'infrastruttura a chiave pubblica, detta PKI [(14)], gestita da un'organizzazione nota come *Autorità di Certificazione* [(15)].

Dal punto di vista tecnologico, la verifica di una firma digitale è un procedimento perfettamente collaudato. Utilizzando i dati forniti in tempo reale dall'Autorità di Certificazione, chiunque può stabilire in maniera facile e sicura chi sia l'autore del documento e se il documento sia stato alterato dopo la firma. Questa almeno è la teoria; la realtà va dipinta in toni nettamente più sfumati. La firma digitale non dimostra, in effetti, che il documento è stato firmato da Tizio. Dimostra che la firma è stata apposta utilizzando un dispositivo (in genere una smart card, simile ad una carta di credito) che è stata in qualche modo consegnata ad una persona che è stata in qualche modo identificata come Tizio [(16)]. La firma digitale, nonostante le sue solidissime fondamenta matematiche e tecnologiche, dipende insomma in modo decisivo dal fattore umano. Se una smart card è ad esempio consegnata alla persona sbagliata [(17)], o se il titolare ne perde il controllo (volontariamente, o per effetto di violenza o frode) la verifica confermerà l'autenticità di un documento che in realtà non proviene affatto da colui che ne risulta essere l'autore. [(18)]

Per queste ragioni le firme digitali apposte dai privati sono considerate meno affidabili di un documento notarile [(19)]. E come si inseriscono in questo contesto le firme digitali apposte dai notai? Occorre, è chiaro, fornire una soluzione convincente alle problematiche appena segnalate.

In primo luogo, ogni notaio di tipo latino è un professionista (forse dovrebbe dirsi *il* professionista) della gestione documentale, abitualmente supportato da una consistente organizzazione d'ufficio, ed è quindi nelle condizioni di adottare ogni precauzione necessaria [(20)] onde evitare falle sul piano della sicurezza. Il paragrafo 1.2.9 del Codice Deontologico dei Notai Europei, come integrato a Monaco nel 2002 [(21)], contiene una specifica previsione a tal proposito, e stabilisce inoltre che i notai europei debbono sempre utilizzare personalmente i propri dispositivi di firma digitale.

Queste precauzioni possono efficacemente completare la sicurezza intrinsecamente offerta dalla tecnologia, ma non risolve i problemi connessi all'affidabilità dell'Autorità di Certificazione. Non solo: una volta stabilita l'identità del sottoscrivente, chi garantisce che egli sia davvero un notaio nella pienezza delle sue funzioni? Detto in termini appena diversi: come possiamo essere certi che quel determinato documento pervenuto via mail (ad esempio: una procura) sia davvero un atto notarile e possa essere utilizzato come tale in un altro Paese?

Le organizzazioni notarili europee hanno dato soluzione a questi problemi per vie diverse. L'Italia è stato il primo Paese a misurarsi con la creazione di un'infrastruttura di firma digitale per i notai, ed ha comprensibilmente scelto la soluzione più semplice e robusta, la cosiddetta FCA (*Flat Certification Authority*): un'Autorità di Certificazione posseduta dai notai e che accetta quali clienti solo notai in carica [(22)]. Le firme possono essere utilizzate solo

nell'esercizio delle funzioni ufficiali, e se il notaio cessa dalla carica per qualunque motivo, il Presidente del Consiglio Notarile revoca immediatamente il certificato di firma. In altri Paesi (la Francia, ad esempio), i notai posseggono un'Autorità di Certificazione la quale però rilascia certificati sia a notai che ad altre figure professionali: la qualifica d'ognuno è indicata nel certificato stesso [(23)]. Ovunque sono state definite procedure rigorose per garantire che il dispositivo di firma sia rimesso personalmente al notaro; in alcuni Paesi (è il caso di Spagna ed Italia, ad esempio) la consegna è personalmente eseguita dal Presidente, che conosce personalmente ogni notaio del suo distretto [(24)].

Queste differenze strutturali contribuiscono a rendere la circolazione internazionale degli atti notarili elettronici una questione complicata.

3. Questioni strategiche in tema di verifica delle firme

Ogniqualvolta una firma elettronica è impiegata in una transazione a rilevanza giuridica, il processo di verifica (come più sopra tratteggiato) è un indispensabile componente della concatenazione di elementi su cui riposa l'affidamento dell'utente. Senza un'analisi tecnica non si può stabilire se sussista l'indispensabile connessione logica tra firma e documento firmato. Senza controllare la validità del certificato con un'interrogazione ad hoc, non si può fare affidamento sull'identità del sottoscrivente. Per tale ragione, ogni documento in ingresso nei pubblici registri tedesco ed italiano è automaticamente sottoposto a tali verifiche non appena il server lo riceve [(25)]. Il funzionario competente ha a sua disposizione tutti i dati relativi al processo di verifica; se l'esito è negativo, la pratica sarà rifiutata per motivi formali [(26)].

Tali esigenze sono ben presenti a chi ha una conoscenza appena approfondita della tecnologia di firma. Le soluzioni possono essere di non così agevole attuazione, specie per l'utente di esperienza non superiore alla media.

3.1 Molteplicità dei formati

Dal punto di vista tecnico, la verifica delle firme è una delle funzionalità offerta da ogni programma utilizzato per la realizzazione delle firme stesse. I primi programmi apparsi sul mercato si preoccupavano soprattutto di verificare correttamente le firme apposte con il medesimo programma, e sin qui non sorgevano inconvenienti di rilievo. Ma quando si provava a verificare firme apposte con altri programmi gli errori si verificavano con una frequenza che lasciava disorientati anche gli utenti più esperti. Da tempo sono in vigore standards che coprono svariati aspetti della tecnologia di firma [(27)], e gli sviluppatori software invariabilmente affermano di operare nel pieno rispetto degli standards stessi. Nonostante ciò la maledizione di Babele regnava sovrana, ed i prodotti di firma si rivelavano tra loro incompatibili anche a livello nazionale. Questo si è rivelato un grande ostacolo per l'uso quotidiano della tecnologia di firma [(28)]. Il nocciolo del problema risiede nell'eccessivo margine che gli standards lasciano all'interpretazione: in assenza di organi di supervisione, ogni fornitore di software è in pratica

libero di affermare, non smentito, che la propria soluzione è quella tecnicamente preferibile e più fedele allo standard.

La situazione è migliorata con la seconda generazione di prodotti di firma, almeno quelli conformi allo standard PKCS. Vari gruppi di sviluppatori raggiunsero accordi su come interpretare gli standards, e questo attenuò i problemi sopra segnalati [(29)]. Sfortunatamente, nessuna di queste specifiche ha conseguito un sufficiente riconoscimento a livello internazionale [(30)]. L'interoperabilità rimane quindi, anche all'interno dell'Unione Europea, una questione critica, che non è ancora stata oggetto di particolare attenzione in quanto le firme digitali sono molto raramente impiegate in contesti transfrontalieri.

Negli anni successivi sono apparse nuove applicazioni basate su standard consolidati: si tratta soprattutto di applicazioni basate sullo standard XML e di firme inserite nel corpo di files di tipo PDF. Tali formati di firma non sono però ancora adottati su larga scala. I formati PDF hanno perlopiù strutture fortemente proprietarie che confinano gli utenti ai prodotti di determinate case software e dei relativi partners commerciali.

3.2 Differenze nei certificati di firma

L'interoperabilità è carente anche per quanto concerne i certificati di firma. Indipendentemente dal luogo ove i certificati stessi sono conservati [(31)], chi si accinge a creare applicazioni a carattere internazionale deve fronteggiare più di una difficoltà.

Il contenuto dei certificati è sostanzialmente uniforme: X503 è un formato ampiamente accettato, e le applicazioni che lo adottano non hanno in genere alcuna difficoltà ad estrarre dal certificato i dati essenziali, come ad esempio il nome del titolare e dell'Autorità emittente.

Non che manchino però i profili critici. I caratteri non sono trattati in maniera omogenea e sorgono quindi problemi con alcune lingue: è il caso della dieresi, molto utilizzata in tedesco, e di alcuni segni tipici delle lingue est europee, che vengono spesso resi con un incomprensibile guazzabuglio di caratteri che disorienta gli utenti. Per lo più mancano poi informazioni intorno alle procedure impiegate dal certificatore, soprattutto per quanto concerne l'identificazione del titolare. Alcune procedure sono estremamente rudimentali: ad esempio alcune Autorità di certificazione considerano sufficiente per una valida identificazione il fatto che sia stata usata online una carta di credito emessa a nome del richiedente il certificato; all'opposto alcune Autorità esigono che la domanda d'emissione di certificato sia autenticata, e consegnano personalmente la smart card al richiedente. Queste informazioni sono essenziali per stabilire il grado di attendibilità del certificato.

L'identità della persona spesso non è sufficiente per la gestione di procedure documentali automatizzate a valore legale: occorre accertare ruoli, qualifiche e posizioni ricoperte, rispetto alle quali le generalità del sottoscrivente talvolta passano addirittura in secondo piano [(32)]. Le qualifiche non rilevano solo nel settore pubblico: pensiamo ai rappresentanti di società od ai procuratori. I certificati possono contenere informazioni attendibile a tale riguardo ed aggiungere sicurezza alle transazioni elettroniche. Purtroppo in questo specifico settore gli

standard disponibili sono persino più frammentari che altrove, e la loro adozione segue a macchia di leopardo. I principali quesiti tuttora aperti sono:

- quali procedure vengono impiegate per accertare le qualifiche del titolare?
- come sono coinvolte nel procedimento le autorità che sarebbero chiamate ad attestare tali qualifiche in un contesto tradizionale?
- come si garantisce da parte del certificatore che la qualifica è rimasta valida dopo l'emissione del certificato? I certificati digitali offrono una preziosa opportunità di mantenere aggiornati simili dati, il che costituisce un vantaggio rispetto al documento cartaceo. Gli archivi dei certificati debbono essere tenuti a tale scopo meticolosamente aggiornati. Le metodiche all'uopo adottate da ciascuna Autorità di Certificazione non sono in genere trasparenti per l'utente finale. Nei vari sistemi giuridici sono anche richiesti diversi livelli di diligenza.

Dal punto di vista tecnico, vi sono diversi metodi per aggiungere informazioni personali ad un certificato: possono essere integrate nel certificato stesso oppure contenuto in un certificato separato, detto certificato d'attributo. Alcune Autorità di Certificazione offrono determinati tipi di certificati solo a quanti appartengono ad un gruppo predeterminato, presumendo che le parti interessate siano al corrente di tale circostanza senza che sia necessario fornirne espressa indicazione.

Come accade con i formati di firma, questi metodi sono utilizzati promiscuamente anche all'interno del medesimo Paese, soprattutto in quelli più grandi, ove il mercato dei servizi di certificazione ha già avuto una qualche forma di evoluzione. La comparazione internazionale conduce a risultati ancora più eterogenei. (33)

Le differenze linguistiche e nel campo delle tradizioni giuridiche recano il loro ulteriore contributo di confusione: funzioni e professioni dal nome simile non sempre hanno nei vari Paesi eguali funzioni e competenze (34).

3.3 Marcature temporali

Nell'ambito delle tecnologie di firma, uno dei concetti meno accessibili ai non specialisti è quello di marcatura temporale, ed altrettanto difficile risulta comprendere perché la marcatura temporale sia spesso una necessità. Le firme contengono la data ed ora di esecuzione. Tali informazioni sono agevolmente falsificabili, giacché derivano dall'orologio interno del computer, che l'utente può manipolare a piacimento. Si possono quindi agevolmente creare firme apparentemente valide con certificati scaduti o revocati.

Nei vari Paesi si danno risposte diverse a questo problema. In alcuni casi le firme basate su un certificato che al momento della verifica si rivela scaduto o revocato sono considerate tout court inattendibili (35). In altre giurisdizioni si ritengono tali documenti validi, in linea di principio, ancorché soggetti ad una sorta di decadimento nel tempo della loro attendibilità (36).

Data ed ora di firma sono attendibili solo se una marcatura temporale viene aggiunta alla firma (37). Con ciò si sostituiscono la data e l'ora risultanti dai settaggi del computer usato con

la firma, e di cui non è documentata la correttezza, con un'informazione proveniente da un server apposito [38]. Anche le marche temporali sono però realizzate con tecniche diverse che ne complicano la verifica. [39]

3.4 Analisi dei risultati

Per l'utente medio, così come per quello avanzato, lo stato dell'arte, sia sotto il profilo tecnico che sotto quello legale, è oscuro, ed a tratti impenetrabile [40]. Ne deriva che la possibilità di ricorrere alle firme elettroniche nelle operazioni transfrontaliere è seriamente limitata. Se l'utente non procede alla verifica della firma, l'affidabilità della firma stessa è drasticamente ridotta. Potrebbe rivelarsi possibile creare un sottoinsieme di regole tecniche da utilizzare in un determinato segmento del mercato, così dando vita ad un nuovo substandard. L'assenza di coordinamento tra i formati di firma e di certificato diffusi sul mercato europeo è un'altra causa di frustrazione per l'utente finale.

4. Possibili soluzioni

4.1 Standards più dettagliati

In casi analoghi è frequente l'auspicio di standard più chiari e rigorosi, che riducano la variabilità delle implementazioni tecniche. L'esperienza dimostra che questa soluzione non produrrebbe probabilmente risultati a breve termine.

Gli standard di firma elettronica esistono da parecchio tempo, ma nessuno è finora riuscito a renderli stringenti in misura tale da consentire ai programmatori di sviluppare applicazioni capaci di funzionare su un'ampia varietà di firme. Vi sono poche speranze che le legislazioni nazionali e la normativa europea possano offrire un utile contributo. I legislatori sono stati molto riluttanti a fissare d'autorità formati o standard, temendo che ciò potesse costituire un ostacolo allo sviluppo tecnico, ed hanno dunque preferito restare tecnologicamente neutri. [41] Non si attende nessun cambiamento di rilievo sul fronte della Direttiva europea. In determinati settori, sono stati compiuti significativi progressi in passato (è il caso della specifica *CommonPKI*, già *ISIS/MTT* [42]), che ha contribuito a migliorare la situazione in Germania; in Italia qualunque Autorità di Certificazione è in grado di gestire qualunque firma digitale italiana [43]). Sinora queste iniziative hanno però lasciato tracce trascurabili a livello internazionale. L'esperienza mostra che non è decisivo lo sviluppo degli standards, ma la loro adozione. Le ragioni del successo di *CommonPKI* sono state principalmente la messa a disposizione di un *testbed*, e cioè di un meccanismo che i programmatori potevano usare per verificare ufficialmente la conformità allo standard dei loro prodotti, nonché un certificato di conformità rilasciato dall'Autorità preposta [44] Tale certificato ha assunto grande importanza anche a livello di marketing. [45]

Sul mercato internazionale, pur quantitativamente non molto significativo nel suo complesso, si affrontano molti operatori diversi e numerosi soggetti a vario titolo interessati.

Le differenze tecniche tra i mercati americano ed europeo non fanno che peggiorare la situazione; negli USA, in particolare, lo sviluppo dei prodotti è pesantemente influenzato dall'esistenza di software proprietario che fa capo a pochissimi produttori. [46]

Per quanto concerne il riconoscimento internazionale dei certificati vi sono progetti come *European Bridge CA*, [47] che puntano all'interconnessione degli archivi dei certificati. Ogni partecipante al progetto accetta i certificati rilasciati dagli altri partecipanti sulla base di determinati standard che vengono accettati al momento dell'adesione. Ancora una volta, lo scarso numero di aderenti ha fatto sì che il progetto abbia recato scarso beneficio. [48] Ciò è probabilmente da addebitarsi, almeno in parte, al fatto che il progetto si basa su strutture di tipo privato: i costi non trascurabili e una forte connotazione nazionale (i partecipanti sono in nettissima maggioranza tedeschi) hanno limitato molto la platea dei partecipanti ed hanno fatto sì che il progetto sia dominato da Autorità di Certificazione commerciali.

4.2 Applicazioni locali

A lungo termine è discutibile, sia dal punto di vista microeconomico che macroeconomico, se si possa fare affidamento su applicazioni locali (che funzionano cioè direttamente sul computer dell'utente) per verificare firme di varia provenienza. Sino ad oggi tali programmi non hanno avuto un mercato particolarmente ampio, e i produttori sono per lo più imprese di medie dimensioni o piccole sussidiarie delle aziende maggiori. [49]

Per operatori di tali dimensioni, è a dir poco impegnativo sviluppare prodotti capaci di operare su un'ampia gamma di firme e di certificati che provengono da contesti nazionali e tecnici diversi. Molti non dispongono delle risorse necessarie a sviluppare e mantenere aggiornate le varianti tecniche. Inoltre, i parametri operativi delle Autorità di Certificazione evolvono costantemente. I certificati e gli algoritmi sono incessantemente soggetti a modifiche ed upgrades, le vecchie versioni vengono poste fuori servizio, e gli strumenti di verifica debbono essere costantemente aggiornati per restare al passo. Gli investimenti necessari, specie in ambito internazionali, appaiono esagerati ed economicamente non convenienti per le aziende più piccole. [50] In termini più generali, non pare avere molto senso che ogni produttore di software crei al suo interno strutture parallele con il relativo know-how, moltiplicando, tra l'altro, la possibilità che il prodotto contenga errori od imperfezioni.

4.3 Un approccio alternativo: la piattaforma di verifica online

Si è già ricordato come le organizzazioni notarili siano stati da tempo all'avanguardia nell'impiego delle firme elettroniche. Sin dalla metà degli anni Novanta si è dibattuto delle firme elettroniche in relazione all'evoluzione dell'atto notarile dal supporto cartaceo alla forma elettronica. [51]

Al volgere del millennio, i notai sono stati in molti Paesi la prima categoria professionale ad adottare le tecnologie di firme elettroniche su larga scala, ed hanno iniziato a creare proprie Autorità di Certificazione per il rilascio dei certificati ai notai. [52] Col diffondersi dell'uso dello

strumento si sono in misura via via crescente scambiate esperienze tra le organizzazioni notarili europee, all'interno dell'associazione paneuropea CNUE. (53)

Gruppi di lavoro interni hanno iniziato a farsi promotori dell'adozione delle tecnologie di firma elettronica su base continentale, basandosi sulle applicazioni nazionali (ad esempio i registri commerciali in Germania, Italia e Spagna) e progettando applicazioni internazionali. Le firme elettroniche hanno rapidamente guadagnato il centro dell'attenzione. La circolazione internazionale dei documenti notarili, procure soprattutto, fa da sempre parte della comune pratica notarile. Il gruppo di lavoro ha finito col convincersi che, all'inverso di quanto era lecito attendersi, la transizione al medium elettronico crea più problemi di quanti non ne risolva (54). Verificare documenti elettronici provenienti dall'estero non è più semplice per il notaio di quanto non sia per ogni altro utente: le incompatibilità a livello software sono le medesime. Si decise quindi di studiare in profondità il problema onde pervenire poi ad una soluzione.

Un sondaggio tra i notariati europei ha confermato quanto si immaginava: le modalità con cui la firma digitale è stata implementata nei vari Paesi diverge a volte in modo assai significativo. Nonostante i sistemi fossero, almeno in buona misura, conformi agli standards, la verifica transfrontaliera delle firme non era possibile.

Venne dapprima proposto lo sviluppo di un programma unico di verifica. L'idea è stata rapidamente accantonata a causa della vastità dell'impegno richiesto per installare e mantenere aggiornato tale software presso molte migliaia di studi notarili in Europa. Sarebbe stato difficile anche individuare una base per lo sviluppo del programma, attesa l'eterogeneità del parco macchine installato, specie per quanto riguarda i sistemi operativi. Un'alternativa ragionevole, si concluse, sarebbe stata la creazione di un servizio online, capace di eseguire la verifica della firma indipendentemente dal sistema operativo impiegato dall'utente e senza richiedere la previa installazione di un software. I notariati spagnoli ed italiano avevano già realizzato sistemi analoghi ad uso domestico, con buoni risultati; in breve tempo i membri del gruppo di lavoro hanno unanimemente abbracciato questa opzione. (55)

4.3.1 Premesse

I componenti del gruppo di lavoro hanno preventivamente concordato alcune condizioni irrinunciabili per il successo del progetto:

- il sistema di verifica avrebbe verificato solo le firme dei notai europei di diritto latino, onde mantenere la complessità tecnica ed organizzativa ad un livello accettabile;
- i profili tecnico informatici del progetto sarebbero stati curati dalle aziende informatiche di proprietà delle organizzazioni notarili dei Paesi partecipanti. Si tratta di società che posseggono tutte un ottimo livello di esperienza nel campo delle firme elettroniche e conoscono in profondità i sistemi di firma impiegati in ciascun Paese;
- le organizzazioni notarili avrebbero fornito il necessario supporto giuridico in relazione alle normative vigenti in ciascun Paese, ed eseguito la traduzione del sito nelle varie lingue;

- non sarebbe stato fornito alcun servizio di certificazione in senso stretto, giacché la soluzione proposta non prevede la creazione di un database autonomo. Ogni richiesta di verifica sarebbe stata eseguita utilizzando i dati forniti dalle rispettive Autorità di Certificazione, così riducendo il rischio di risposte errate, potenziale fonte di responsabilità; in altri termini, il sistema funziona come una sorta di ripetitore delle informazioni giuridicamente rilevanti.

4.3.2 Obiettivi del progetto

I partecipanti hanno diretto i loro sforzi verso questi obiettivi:

- la piattaforma deve essere in grado di analizzare i dati ricevuti e di riconoscere automaticamente il tipo di firma, così individuando la tecnica di verifica da utilizzare. il server cui richiedere le informazioni relative al certificato e le modalità con cui inoltrare la richiesta. All'utente si richiede soltanto di sottoporre il documento da verificare;
- i risultati debbono essere presentati in un modo adatto all'utente mediamente esperto, consentendogli di percepire in maniera immediata se la firma è attendibile o meno. I dettagli debbono essere resi disponibili immediatamente, se richiesti;
- per assicurare la migliore comprensione, l'interfaccia utente e la presentazione dei risultati debbono essere offerti nella lingua dell'utente. Sempre nella lingua dell'utente, debbono essere rese disponibili informazioni circa le peculiarità giuridiche delle firme elettroniche nel sistema giuridico del Paese di provenienza;
- oltre ad informazioni attendibili sull'identità del sottoscrivente, deve espressamente indicarsi se il sottoscrivente era notaio al momento della sottoscrizione. Ciò consente all'utente di stabilire se il documento in suo possesso ha natura di atto autentico elettronico;
- il sito pone infine a disposizione dell'utente materiali informativi sul contesto normativo di riferimento, attraverso links a risorse giuridiche disponibili online, come ad esempio testi di legge sulle firme elettroniche e sull'attività notarile.

Raggiunti questi obiettivi, la piattaforma di verifica per le firme dei notai europei potrà probabilmente proporsi come un esempio di architettura semplice ed user-friendly in materia di verifica di firme elettroniche.

4.4 Attuale stato d'avanzamento del progetto

Nel 2005 il gruppo di lavoro comprendeva i Paesi interessati a sviluppare gli aspetti tecnici ed editoriali della piattaforma di verifica: le organizzazioni notarili di Germania, Spagna, Francia ed Italia. Il notariato austriaco ha partecipato quale osservatore sin dal principio dei lavori. Nella prima metà del 2006 sono state eseguite diverse inchieste presso le organizzazioni notarili interessate per ottenere un quadro d'insieme sufficientemente dettagliato dei differenti approcci tecnici utilizzati nei singoli Paesi, e di ciò che ne derivava in termini di lavoro da compiere. A metà di quell'anno si era raggiunto un unanime consenso sulla fattibilità del

progetto, e la seconda metà di quell'anno fu occupata dall'elaborazione delle linee fondamentali del software e dall'installazione dell'infrastruttura.

Sembra degno di nota che un'operazione di questo livello di complessità sia stata efficacemente realizzata distribuendo le mansioni tra quattro diverse organizzazioni in quattro diversi Paesi. I vari team si sono tenuti in contatto per via elettronica; i rispettivi leaders si riunivano molto frequentemente in videoconferenza, risolvendo i problemi che via via si presentavano e ripartendo il lavoro tra i vari Paesi. Un altro aspetto interessante è la composizione del gruppo di lavoro internazionale: un mix di tecnici informatici e di notai interessati all'informatica: è stato così risolvere ad un tempo, ed in modo coordinato, sia i problemi tecnici che quelli giuridici.

Il prototipo è stato reso disponibile per uso interno alla CNUE all'inizio del 2007, e presenta già tutte le principali caratteristiche del prodotto definitivo:

- il servizio è accessibile a tutti via Internet e funziona indipendentemente dal sistema operativo e dal browser utilizzato;
- il sistema di verifica è in grado di verificare documenti firmati elettronicamente da notai in Francia, Italia, Spagna e Germania;
- sono disponibili due opzioni: il documento può essere inoltrato (attraverso un *upload*) al sito web oppure, se ragioni di privacy o legate alle dimensioni del documento lo rendono preferibile, è possibile scaricare un *Java applet* che esegue l'operazione di verifica in locale evitando di far viaggiare dati riservati;
- ai certificati si accede sempre direttamente presso il sistema dell'Autorità di Certificazione emittente;
- i risultati della verifica sono presentati in maniera ordinata ed utilizzando colori guida: se la firma è inattendibile i risultati della verifica sono presentati a sfondo rosso; lo sfondo verde indica firme attendibili; lo sfondo giallo attira l'attenzione dell'utente su situazioni dubbie. In quest'ultimo caso, viene presentata in video all'utente una dettagliata spiegazione;
- altre pagine web del sito offrono ulteriori informazioni sulle firme elettroniche;
- il servizio è costruito in modo modulare. Nuove tipologie di firma possono essere aggiunte senza eccessive complicazioni. Diversi notariati europei hanno già manifestato interesse in tal senso.

Durante il 2007 il prototipo è stato presentato a diverse conferenze, soprattutto nell'ambito delle istituzioni europee, con positiva accoglienza e diffuse manifestazioni di interesse [(56)]. Il progetto è già annoverato tra i progetti di riferimento in un'iniziativa paneuropea sull'e-Justice che comprende il progetto di un portale internet.

L'iniziativa dei notai europei ha fatto emergere un'alternativa a soluzioni più proprietarie offerte dai maggiori operatori internazionali.

Nel frattempo, il gruppo di lavoro sta eseguendo interventi migliorativi di dettaglio sul sito ed ha iniziato a lavorare sull'integrazione di un maggior numero di varianti di firma. Gli

organi competenti della CNUE stanno attualmente valutando se fornire il servizio ai soli notai, ai tribunali, ad altre autorità pubbliche od alla generalità del pubblico.

5. Conclusioni: uno sguardo al futuro

La piattaforma CNUE renderà i notai europei intercambiabili? Vedremo ad esempio un notaio parigino ricevere l'atto di vendita di un immobile a Vienna ed eseguire tutte le successive formalità presso i pubblici uffici via Internet?

La risposta è un netto "no". L'identificazione delle parti non è il principale compito del notaio latino. Egli è responsabile per tutta una serie di questioni che ruotano intorno al contratto. Se il venditore si rivela non essere il legittimo proprietario dell'immobile, il notaio sarà tenuto a rifondere il danno. Lo stesso accade se il notaio non identifica correttamente eventuali ipoteche. Il notaio deve accertare che i termini contrattuali siano conformi ad ogni possibile norma di legge. Deve illustrare alle parti il significato, gli effetti giuridici e le conseguenze del contratto. Nella maggior parte dei paesi, deve riscuotere le imposte dovute sul contratto, ed è responsabile verso l'Amministrazione Tributaria per eventuali manchevolezze. In alcuni Paesi, un notaio viene addirittura reputato responsabile laddove non abbia informato gli interessati di un'agevolazione tributaria cui le parti avevano diritto [(57)]. Il notaio può essere ritenuto responsabile anche in qualche ipotesi di illecito urbanistico. Se una somma di denaro appare di provenienza illecita, le competenti autorità ne vengono informate.

Queste funzioni sono svolte non solo nell'interesse delle parti, ma anche e soprattutto nell'interesse pubblico, giacché contiene la litigiosità a livelli incredibilmente modesti [(58)] in tutti i settori ove il notaio opera. Come si è osservato [(59)], il notaio è la *title insurance* del diritto latino, e molto altro.

Un simile ruolo può essere svolto solo da un professionista competente e Pubblico Ufficiale (il notaio latino possiede entrambe queste qualità) che abbia approfondita conoscenza della legislazione locale, e che sia in grado di cooperare con le pubbliche amministrazioni del proprio Paese. Se i sistemi giuridici europei saranno un giorno così integrati da rendere le differenze nazionali semplici sfumature, solo allora la nascita di un'unica professione giuridica paneuropea sarà una logica conseguenza. Sino a quel momento (se mai si verificherà) vivremo in un sistema basato su notariati nazionali, ognuno dei quali si occuperà delle vicende giuridiche del proprio Paese.

Per queste ragioni è ragionevole prevedere che, almeno in una prima fase, la piattaforma CNUE faccia circolare prevalentemente procure. Il notaio locale resterà responsabile dell'atto, mentre i notai degli altri Paesi si occuperanno delle procure che saranno rilasciate dalle persone che non vorranno o non potranno recarsi presso il primo notaio per la stipula dell'atto. In alternativa si può ipotizzare che l'atto sia preparato dal notaio locale, unico responsabile della sua conformità all'ordinamento del luogo, e firmato elettronicamente da una parte dinanzi al medesimo notaio e dall'altra parte dinanzi ad un notaio straniero.

Anche per i documenti in formato digitale, dovranno in ogni caso rispettarsi le vigenti regole in materia di legalizzazione degli atti. All'interno dell'Unione Europea la legalizzazione in molti casi non è più richiesta: esistono svariati accordi bilaterali in tal senso ed uno multilaterale, firmato il 25 maggio 1987 a Bruxelles, attualmente (settembre 2008) in vigore tra Belgio, Cipro, Danimarca, Francia, Italia, Irlanda e Lettonia.

Se nessuno di tali accordi risulta applicabile alla fattispecie, sarà necessaria l'Apostille secondo la convenzione dell'Aja del 1961 [(60)], ovviamente nella sua versione elettronica: la e-Apostille. In sintesi, la e-Apostille è un file (o una porzione di un file) che reca le medesime informazioni contenute in un'Apostille, da essere allegato all'atto pubblico od autenticato

La Conferenza Permanente dell'Aja per il Diritto Internazionale Privato [(61)] nel cui ambito venne elaborata la Convenzione del 1961, sostiene con convinzione l'e-Apostille sin dal 2005. In quell'anno venne tenuta a tal proposito un'importante conferenza a Las Vegas, organizzata congiuntamente all'UINL [(62)] ad alla NNA [(63)]; successivamente si sono tenuti forum in argomento a Washington (2006), Los Angeles (2007) e New Orleans (2008). I documenti unanimemente adottati da tali conferenze dichiarano ufficialmente che nessuna previsione della convenzione impedisce che la Apostille sia emessa in formato elettronico. La Conferenza ha adottato un atteggiamento "*technology neutral*": ogni tecnologia idonea può essere utilizzata, e la firma digitale è la candidata meglio qualificata. L'e-Apostille sarà insomma nient'altro che un ulteriore documento provvisto di firma digitale, e la piattaforma CNUE potrà gestirle agevolmente, come è già stato dimostrato nella Conferenza e-Justice indetta dalla presidenza slovena di turno dell'Unione nel giugno 2008 a Portorose.

Ugo Bechini e Dominik Gassen [(**)]

(*) La circolazione internazionale di documenti notarili in forma elettronica, almeno all'interno dell'Europa, si avvia a diventare presto una realtà grazie alla piattaforma IVTF creata in ambito CNUE, ed attualmente operativa, in regime di betatest, presso Notartel in Roma. Il lavoro costituisce il primo tentativo di illustrazione di un sistema con cui i notai italiani dovranno con ogni probabilità confrontarsi già nel prossimo futuro. Il testo è apparso in originale sul *Michigan State University Journal of International Law* (http://www.law.msu.edu/jil/) volume 17 (2008/2009) Issue 3, in traduzione tedesca su *DuD - Datenschutz und Datensicherheit* (http://www.dud.de – Wiesbaden), fascicolo 10/2008 e nella traduzione italiana che qui, per cortese concessione, si riproduce, su *Il diritto dell'informazione e dell'informatica*, n. 2/2009.

Lo scritto contiene riferimenti ai sistemi giuridici di *civil law* del tutto superflui per il lettore italiano, che sono stati tuttavia conservati per salvaguardare il carattere internazionale del lavoro. Ove non diversamente indicato, i riferimenti in nota a legislazione, giurisprudenza e dottrina italiane non costituiscono adattamenti di questa traduzione ma sono direttamente tratti dall'originale inglese. (N.d.A.)

(**) D. Gassen è Notaio in Bonn, Coordinatore dell'IVTF (International Verification Task Force) in seno alla CNUE (Conferenza dei Notariati dell'Unione Europea); U. Bechini è Notaio in Genova, già Coordinatore dell'IVTF ed attualmente Chairman del Gruppo di Lavoro Nuove Tecnologie presso la CNUE.

1) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20000119:IT:PDF.

Una visione d'insieme della direttiva in Francisco Javier GARCÍA MAS, *Comercio y firma electrónicos*, Lex Nova, Valladolid 2004 (seconda edizione), p. 37.

2) Secondo la direttiva di cui alla nota precedente, i certificati qualificati devono includere:

- *l'indicazione che il certificato rilasciato è un certificato qualificato;*
- *l'identificazione e lo Stato nel quale è stabilito il prestatore di servizi di certificazione;*
- *il nome del firmatario del certificato o uno pseudonimo identificato come tale;*
- *l'indicazione di un attributo specifico del firmatario, da includere se pertinente, a seconda dello scopo per cui il certificato è richiesto;*
- *i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario;*
- *un'indicazione dell'inizio e del termine del periodo di validità del certificato;*
- *il codice d'identificazione del certificato;*
- *la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato;*
- *i limiti d'uso del certificato, ove applicabili; e*
- *i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili.*

Inoltre, i prestatori di servizi di certificazione che rilasciano certificati qualificati devono:

(a) dimostrare l'affidabilità necessaria per fornire servizi di certificazione;

(b) assicurare il funzionamento di un servizio di repertorizzazione puntuale e sicuro e garantire un servizio di revoca sicuro e immediato;

(c) assicurare che la data e l'ora di rilascio o i revoca di un certificato possano essere determinate con precisione;

(d) verificare con mezzi appropriati, secondo la legislazione nazionale l'identità e, eventualmente, le specifiche caratteristiche della persona cui è rilasciato un certificato qualificato;

(e) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi forniti, in particolare la competenza a livello gestionale, la conoscenza specifica nel settore della tecnologia delle firme elettroniche e la dimestichezza con procedure di sicurezza appropriate; essi devono inoltre applicare procedure e metodi amministrativi e i gestione adeguati e corrispondenti a norme riconosciute;

(f) utilizzare sistemi affidabili e prodotti protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti di cui sono oggetto;

(g) adottare misure contro la contraffazione dei certificati e, nei casi in cui il prestatore di servizi di certificazione generi dati per la creazione di una firma, garantire la riservatezza nel corso della generazione di tali dati;

(h) disporre di risorse finanziarie sufficienti ad operare secondo i requisiti previsti dalla direttiva, in particolare per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione;

(i) tenere una registrazione di tutte le informazioni pertinenti relative ad un certificato qualificato per un adeguato periodo di tempo, in particolare al fine di fornire la prova della certificazione in eventuali procedimenti giudiziari. Tali registrazioni possono essere elettroniche;

(j) non conservare né copiare i dati per la creazione della firma della persona cui il prestatore di servizi di certificazione ha fornito i servizi di gestione della chiave;

(k) prima di avviare una relazione contrattuale con una persona che richieda un certificato a sostegno della sua firma elettronica, informarla con un mezzo di comunicazione durevole, degli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e i risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte e utilizzare un linguaggio comprensibile. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;

(l) utilizzare sistemi affidabili per memorizzare i certificati in modo verificabile e far sì che:

- *soltanto le persone autorizzate possano effettuare inserimenti e modifiche;*
- *l'autenticità delle informazioni sia verificabile,*
- *i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato,*
- *l'operatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza.*

3) *Accreditamento facoltativo*, secondo la Direttiva, è *qualsiasi permesso che stabilisca diritti ed obblighi specifici della fornitura di servizi di certificazione, il quale sia concesso, su richiesta del prestatore di servizi di certificazione interessato, dall'organismo pubblico o privato preposto all'elaborazione e alla sorveglianza del*

rispetto di tali diritti ed obblighi, fermo restando che il prestatore di servizi di certificazione non è autorizzato ad esercitare i diritti derivanti dal permesso fino a che non abbia ricevuto la decisione da parte dell'organismo .

4) Secondo la Direttiva, *i dispositivi per la creazione di una firma sicura, mediante mezzi tecnici e procedurali appropriati, devono garantire almeno che:*

1. *i dati per la creazione della firma utilizzati nella generazione della stessa possono comparire in pratica solo una volta e che è ragionevolmente garantita la loro riservatezza;*
2. *i dati per la creazione della firma utilizzati nella generazione della stessa non possono, entro limiti ragionevoli di sicurezza, essere derivati e la firma è protetta da contraffazioni compiute con l'impiego di tecnologia attualmente disponibile;*
3. *i dati per la creazione della firma utilizzati nella generazione della stessa sono sufficientemente protetti dal firmatario legittimo contro l'uso da parte di terzi.*

Infine, i dispositivi per la creazione di una firma sicura non devono alterare i dati da firmare né impediscono che tali dati siano presentati al firmatario prima dell'operazione di firma.

5) Persino un SMS risponde a tali criteri: Stephen MASON, *Electronic Signatures in Law*, Lexis Nexis UK, London 2003, p. 101. Se la firma elettronica è definita infatti come *dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione* (claudicante traduzione *dell'authentication* inglese) è difficile negare che l'indicazione del numero del mittente soddisfi i requisiti.

6) In Italia, ad esempio, il Decreto Legislativo 23 gennaio 2002 n. 10, equiparava i documenti provvisti di firma elettronica, di qualunque tipologia essa fosse, ai documenti scritti. Pertanto persino le vendite immobiliari (che secondo l'articolo 1350 del Codice Civile Italiano possono farsi con semplice scritto, almeno per quanto concerne i rapporti tra le parti) avrebbero potuto essere concluse con un semplice SMS. Una previsione così scricchiolante non poté che attirare su di sé critiche pesanti (*inter alia*, Mario MICCOLI ed Ugo BECHINI, *Attuazione della direttiva europea sulla firma elettronica, ovvero la forma "sine probatione*", Notariato, 2002, 324) e venne più tardi spazzata via dal Decreto legislativo 5 marzo 2005, n. 82.

7) Una breve descrizione in lingua inglese del ruolo del notaio latino è disponibile nella sezione inglese del sito www.notariato.it. Circa il 55% della popolazione mondiale vive in Paesi di notariato latino, ove non operano i Notaries Public anglosassoni. Un'analisi approfondita è quella di Pedro A. MALAVET, *The Non-Adversarial, Extra-Judicial Search for Legality and Truth: Foreign Notarial Transactions as an Inexpensive and Reliable Model for a Market Driven System of Informed Contracting and Fact-Determination, in Wisconsin International Law Journal, Volume 16 Number 1 Winter 1997,* P. 1.

8) *One stop shop nell'originale [NdT].*

9) Ugo BECHINI e Michele NASTRI, *Il notaio e la contrattazione elettronica*, in *Relazioni al XXIV Congresso internazionale del notariato latino. Città del Messico, 17-22 ottobre 2004*, Giuffré 2004. Il testo è disponibile in spagnolo ed italiano, insieme ad un abstract in inglese, alla pagina http://xoomer.alice.it/ubechini/demo/ ove è pure disponibile una demo in inglese, francese ed italiano sull'iter telematico relativo alla costituzione di una società in Italia. Per quanto riguarda invece la procedura telematica di trasferimento degli immobili, si veda Sabrina CHIBBARO, *Usage of information and communications technology in real estate conveyancing: Italian experience* http://www.nationalnotary.org/intlforum/pdf/Forum_3_Chibbaro.pdf, presentazione al Third International Forum on Digital Evidence, Los Angeles 2007.

10) Si usa definire *killer app* uno dei possibili impieghi di una nuova tecnologia, che da solo è però sufficiente ad indurre una massa significativa di utenti ad adottare la tecnologia stessa. L'accesso alle partite di calcio, ad esempio, può essere descritto, almeno in Italia, come la *killer app* della televisione satellitare [NdT].

11) Sin dal pioneristico lavoro di Mario MICCOLI, *Documento e Commercio Telematico*, IPSOA, Milano 1998.

12) Le relazioni nazionali al XXIV Congresso internazionale del notariato latino. Città del Messico 2004, forniscono informazioni interessanti, in particolare quelle francese, tedesca, spagnola, olandese ed italiana. Si veda anche Bernard REYNIS ed Ugo BECHINI, *European Civil Law Notaries ready to launch international digital deeds,* in *Digital Evidence Journal,* vol IV n. 1 (2007) p. 12; un loro precedente contributo sul medesimo argomento è *La firma digitale transfrontaliera dei notai: una realtà europea,* in *Notariato* (IPSOA), 2004 (6) p. 573, simultaneamente apparso in lingua francese, (*La signature électronique transfrontalière des notaires: une réalité européenne), ne La Semaine Juridique, édition notariale & immobilière,* 2004 (39) 1447.

13) La prima legislazione tedesca (Bundesgesetzblatt Teil 1, 1997, p. 1870, 1872)) ed italiana (DPR 10 Novembre1997, n. 513) discorrevano entrambe di firme *digitali*, anziché *elettroniche*.

14) Le voci *Digital Signature e Firma Digitale* di *Wikipedia* forniscono una buona informazione di base; per maggior approfondimento si veda Warwick FORD e Michael S. BAUM, *Secure Electronic Commerce*, Prentice Hall (Upper Saddle River, New Jersey), 2001.

15) Alcune delle funzioni abitualmente svolte dalle Autorità di Certificazione sono talvolta attribuite ad organizzazioni separate, dette *Registration Authorites*. Warwick FORD e Michael S. BAUM, *ibidem*; un'informazione di base è disponibile su *Wikipedia*, voci *Certificate Authority e Registration Authority*.

16) *There are several obvious problems posed by trying to tie the identity described in a digital signature certificate to an actual person with the intention of binding the party thus identified to the content of an electronic record. Among these are:*

- *whether the token/smart card has been deliverd to the right person;*
- *whether the authorized person has used the token with the private key when performing the signature;*
- *and if a person other than the identified person has used the digital signature, how that person was able to gain access without authorization and*
- *who should bear responsibility for that unauthorized access.*

The breach in security may occur at the level of the end user's failure to take reasonable steps to safeguard access to a private key, or it may occur because the software and hardware used to store the private key have not been made reasonably secure. It may even stem from an uninformed attempt of the authorized user to delegate an inconvenient procedure. Before a digital signature can be presumed to be as valuableas a traditional handwritten signature, the behavior, attitudes and sophistication of individuals using the technology will have to be analyzed as well as the security characteristics of the entire system within which an individual digital signature is used. At present, due in part to the lack of standardization among implementations and depth of experience with actual use of digital signature technologies as signatures, that information does not yet exist. In addition, while it may be feasible at present to try to develop and enforce such standards of behavior among participants in a "closed" system in which members agree by contract or system rules on the applicable standards, no one has yet found a feasible way to standardize end user conduct in an "open" environment such as Internet transactions between entities with no prior relationship.

(Collegare l'intestazione di un certificato digitale con l'intento di una ben individuata persona di vincolarsi al contenuto di un documento digitale è operazione che presenta più di un problema. Occorre in particolare stabilire:

- se il dispositivo di firma è stato consegnato alla persona giusta;
- se la il dispositivo di firma è stato utilizzato dal titolare;
- in caso contrario, come una persona diversa dal titolare ha ottenuto accesso al dispositivo, e
- chi deve essere ritenuto responsabile per tale accesso non autorizzato.

Una siffatta breccia nella sicurezza nel sistema può accadere in quanto l'utente finale trascura di osservare le ragionevoli misure di sicurezza, o perché il software e l'hardware utilizzati per conservare la chiave privata non sono sufficientemente sicuri. Può persino derivare dal desiderio di un utente disinformato di delegare una procedura noiosa. Prima che la firma digitale possa essere reputata affidabile quanto quella tradizionale, il comportamento, gli atteggiamenti e la competenza degli individui che impiegano la tecnologia dovranno essere analizzati, e così pure le caratteristiche di sicurezza dell'intero sistema nel cui ambito la firma digitale è impiegata. Queste informazioni non sono oggi disponibili: i sistemi di firma non sono sufficientemente standardizzati e non si è ancora maturata esperienza sull'uso effettivo delle tecnologie di firma digitale come strumento di sottoscrizione Inoltre, se appare attualmente possibile sviluppare simili standard di comportamento nell'ambito di sistemi chiusi, le cui parti aderiscono volontariamente agli standard medesimi, nessuno ha ancora trovato una via che consenta di standardizzare il comportamento degli utenti in un ambiente aperto, come nel caso di transazioni via Internet tra utenti che non hanno avuto contatti precedenti - Jane K. WINN, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, Idaho Law Review, Volume 37, Issue 2, 2001; *traduzione degli autori*).

17) Il 29 ed il 30 gennaio 2001, VeriSign, un'autorità di certificazione californiana, leader mondiale del settore, rilasciò due certificati digitali a due impostori che affermavano falsamente di rappresentare la società Microsoft. Secondo il sito della stessa VeriSign (http://www.verisign.com/support/advisories/authenticodefraud.html, visitato il 17 marzo 2008*) the certificates were VeriSign Class 3 Software Publisher certificates and could be used to sign executable content under the name "Microsoft Corporation". The risk associated with these certificates is that the fraudulent party could produce digitally signed code and appear to be Microsoft Corporation. In this scenario, it is possible that the fraudulent party could create a destructive program or*

ActiveX control, then sign it using either certificate and host it on a Web site or distribute it to other Web sites (i certificati erano VeriSign Class 3 Software Publisher certificates che potevano essere usati per firmare eseguibili col nome "Microsoft Corporation". Il rischio derivante da questi certificati è che gli impostori potevano firmare eseguibili che sarebbero apparsi come provenienti dalla Microsoft. Sarebbe stato possibile agli impostori creare un programma od un controllo ActiveX con effetti distruttivi, firmarlo usando uno dei certificati e collocarlo su un sito web o distribuirlo ad altri siti web - *traduzione degli autori*).

18) Secondo Stephen MASON (*Electronic Signatures* in *Law,* Lexis Nexis UK, London 2003, p. 348) *no form of electronic signature is capable of linking the use of a signature to a particular person. Unless the sending party confirms they sent the message or document with the signature attached, the recipient cannot determine whether the sending party authorized the use of the signature* (nessun tipo di firma elettronica è capace di collegare l'uso della firma stessa ad una determinata persona. A meno che il mittente non confermi di aver inviato il messaggio od il documento provvisto di firma, il destinatario non è in grado di stabilire se il mittente apparente abbia o meno autorizzato l'uso della firma - *traduzione degli autori*).

19) *Digitally-signed documents do not achieve the same assurances of genuineness that documents signed in the personal presence of a notary achieve, and should not be given the same legal status* (La firma digitale non attribuisce al documento una garanzia di autenticità paragonabile a quella dei documenti firmati in presenza del notaio, e non dovrebbe pertanto attribuirsi loro il medesimo status giuridico: Brad BIDDLE, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, San Diego Law Review - 33 - 1143, 1996*; traduzione degli autori*).Per dirla con Michel GRIMALDI e Bernard REYNIS (*L'acte authentique électronique, in Répertorie Defrénois, 15/9/03), levons ici une ambiguïté. Révéler son code à des tiers ou ne pas le protéger de leur indiscrétion peut être une faute d'imprudence ou de négligence, de nature à engager la responsabilité civile de son titulaire. Mais ce n'est pas ce dont il s'agit ici : ici, c'est la réalité du consentement qui est en cause* (liberiamoci di un'ambiguità. Rivelare i propri codici a terzi o non proteggerli da accessi non autorizzati può rappresentare una colpevole imprudenza o negligenza, di cui il titolare può essere considerato responsabile. Ma non di questo ci stiamo occupando; qui è in gioco l'effettività del consenso - *traduzione degli autori*).

20) Il notaio sarà responsabile laddove non adotti le necessarie precauzioni. La maggior parte dei notai latini sono d'altra parte assicurati per la loro responsabilità professionale, con massimali che si misurano in milioni di dollari.

21) Il testo è disponibile in francese e tedesco presso www.cnue.eu (e presso www.notariato.it in italiano NdT).

22) Punto 3.3 del *Manuale Operativo* dell'Autorità di Certificazione dei notai italiani, disponibile presso ca.notariato.it.

23) Punto 2.3.5 del *Manuale Operativo (Politique de Certification)* dell'Autorità di Certificazione dei notai francesi, disponibile presso www.preuveelectronique.org.

24) Punto 4.4 del *Manuale Operativo* dell'Autorità di Certificazione dei notai italiani, disponibile presso ca.notariato.it.

25) Dominik GASSEN e Stefan WEGERHOFF, *Elektronische Beglaubigung und elektronische Handelsregisteranmeldung in der Praxis,* Münster 2007, p. 228. Le procedure automatiche di verifica hanno rapidamente creato serie difficoltà tecniche quando è stata introdotta la prassi di verificare tutti i certificati (quello dell'utente, quello dell'autorità di certificazione e quello root governativo). L'effetto è stato un aumento davvero inaspettato di traffico in direzione dei rispettivi server.

26) Nel sistema tedesco, le firme elettroniche che non conseguono almeno il livello di firma qualificata secondo la normativa europea, non sono in linea di principio ammissibili nelle trasmissioni di documenti a valore legale (ad esempio nei depositi presso i Pubblici Registri, §§ 12 II HGB, 39a BeurkG).

27) L'autorità federale tedesca per la sicurezza informatica (BSI): http://www.bsi.de/esig/standards.htm; Tra gli altri, vanno ricordati gli standards PKCS, standards che coprono una larga varietà di aspetti. Si veda ad esempio, http://en.wikipedia.org/wiki/PKCS.

28) Un buon esempio è la situazione in Germania ed Italia dopo che la prima legislazione in tema di firma digitale venne promulgata nel medesimo anno, il 1997.

29) Un esempio è la specifica *Common PKI (*già *ISIS/MTT)* sviluppata in Germania e che ha consentito una migliore interoperabilità tra li operatori tedeschi http://www.common-pki.org/index.php?id=567&L=1.

30) Neppure Microsoft è riuscita ad assumere la guida del settore, mentre di solito la poderosa quota di mercato detenuta da quella Società fa sì che i suoi standard godano di ampia diffusione. In materia di firme elettroniche, Microsoft ha perseguito una strategia focalizzata esclusivamente sul mercato nordamericano, e le firme europee

apposte a mezzo di smart cards, ancorché perfettamente conformi alla legislazione nazionale ed europea, non vengono riconosciute dalle procedure native di Windows. I prodotti americani, a loro volta, per lo più non sono conformi alla normativa europea.

31) Le smart cards sono molto differenti tra loro per quanto riguarda specifiche tecniche e sicurezza.

32) E' soprattutto il caso di ogni persona che ricopra incarichi pubblici. Le speciali proprietà giuridiche dell'atto notarile derivano ad esempio dal pubblico ufficio ricoperto dal notaio, non dalla sua identità personale.

33) Bundesnetzagentur, http://www.bundesnetzagentur.de/enid/547491ee07d00671e65f8f91463c74a0,0/FAQ/Antwortssss_wm.html.

34) Questo non è un problema peculiare del mondo digitale: lingue e culture giuridiche diverse aggiungono sempre una dose di complessità alle transazioni transfrontaliere. E' forse solo un poco più evidente al palato dei frequentatori del web, abituati a muoversi a livello globale senza barriere di sorta.

35) Tale approccio è prevalente in Italia: fondamentale in materia il contributo di Raimondo ZAGAMI; si veda in particolare *Firma digitale e sicurezza giuridica*, Cedam, Padova 2000, p. 214.

36) Alexander ROSSNAGEL, Stefanie FISCHERDIESKAU, Ulrich PORDESCH, Ralf BRANDNER (2003): *Erneuerung elektronischer Signaturen - Grundfragen der Archivierung elektronischer Dokumente,* in *Computer und Recht*, Heft 4 vom 15. April 2003, 301 – 306; Ulrich PORDESCH, Christian FRYE: *Sicherheitseignung von Algorithmen qualifizierter Signaturen, in DuD (Datenschutz und Datensicherheit)* 2003; 27 (2): 73 - 83. Questo problema è strettamente connesso al settore d'impiego delle firme digitali. Se si tratta di gestire transazioni non destinate a durare nel tempo, l'approccio più rigoroso può essere impiegato, ma se il documento informatico deve essere conservato sul lungo periodo, o deve costituire una fonte di prova, debbono considerarsi altri approcci.

37) In alcuni casi (nel sistema dei notai belgi, ad esempio) ogni firma deve obbligatoriamente essere provvista di una marca temporale.

38) *Wikipedia*, voce *Trusted timestamping.*

39) Le marche temporali possono essere integrate nella firma od essere prodotte come files a parte.

40) Fino ad ora, la tecnologia di firma digitale ha interessato un pubblico relativamente piccolo, che non giustificava investimenti massicci sull'interfaccia utente: lo sviluppo delle applicazioni si è quindi concentrato soprattutto sui profili strettamente tecnici. La legislazione è alquanto disomogenea dei Paesi europei e negli Stati americani, ed ognuno possiede un quadro normativo lievemente differente in tema di firma elettronica, e differenti stati di integrazione delle firme col resto del sistema giuridico. I testi normativi (si prenda ad esempio la situazione connessa alla direttiva europea, *supra* nota 1) presentano sfumature diverse in tema di forme, formati, prerequisiti e conseguenze delle varie tipologie di firma, problematiche anche per i giuristi di professione.

41) Per la situazione in Germania si veda Dominik GASSEN, *Digitale Signaturen in der Praxis*, Köln 2002, p. 148. A posteriori, la saggezza di tale scelta è discutibile. La tecnologia di firma è rimasta sostanzialmente invariata da metà degli anni Novanta; la strategia legislativa ha alimentato la creazione di standard confliggenti, ma non ha affatto stimolato lo sviluppo di nuove tecnologie. L'Unione Europea ha avuto mano più felice, a suo tempo, nel campo della telefonia mobile: lo standard obbligatorio GSM ha garantito un'interoperabilità totale, creando i presupposti per una più dinamica concorrenza in Europa che negli stessi Stati Uniti, il che non avviene poi così di frequente.

42) Cui si è già accennato, nota 29.

43) Per esempio, la piattaforma di verifica dei notai italiani, http://ca.notariato.it/ , può verificare qualunque firma italiana.

44) www.common-pki.org.

45) Nel 2007, tutti i produttori di applicazioni di firma conformi alla legge tedesca supportavano questo standard (si vedano ad esempio http://www.secrypt.de/produkte/digiseal-office/; http://www.seccommerce.com/de/produkte/webcontrust/secsigner/secsigner.html)

46) I protagonisti del mercato sono Microsoft ed Adobe. La prima integra sistemi di firma nei suoi prodotti Windows ed Outlook; in passato, ha strettamente cooperato con Verisign. Adobe ha integrato le funzioni di firma in versioni proprietarie del formato PDF, tipiche della linea di prodotti Acrobat.

47) http://www.bridge-ca.org.

48) Si veda la lista dei partecipanti presso https://www.bridge-ca.org/html/partners.html.

49) Questo è vero soprattutto per la Germania, ove i maggiori providers sono SecCommerce, OpenLimit e Secrypt, tutte aziende piuttosto piccole. Deutsche Post e Deutsche Telekom sono sul mercato come Autorità di Certificazione, ma non si occupano di produrre applicazioni di firma.

50) I produttori di software tedeschi hanno avuto difficoltà ad allocare le risorse necessarie a realizzare le frequenti evoluzioni tecnologiche che sono state richieste dalle autorità pubbliche. L'integrazione dei certificati Austriaci e Svizzeri ha rappresentato un importante progresso per SecCommerce (http://www.seccommerce.com/de/produkte/smartcards/smartcards.html).

51) Jörg BETTENDORF, EDV und Internet in der notariellen Praxis, Köln 2002; Dominik GASSEN, DNotZ 2006, p. 582.

52) In Germania: Zertifizierungsstelle der Bundesnotarkammer; in Francia real. not; in Spagna ANCERT; in Italia il Consiglio Nazionale del Notariato.

53) www.cnue.eu. Entrambi gli autori fanno parte, sin dalla sua fondazione, del gruppo IVTF (International Verification Task Force) che il notariato europeo (CNUE) ha delegato a curare le materie oggetto di questo articolo. Le informazioni relative al progetto discusso nel testo sono pertanto di diretta conoscenza degli autori e non sono state precedentemente pubblicate.

54) Si veda ad esempio la legislazione tedesca, EHUG: http://www.bgblportal.de/BGBL/bgbl1f/bgbl106s2553.pdf. In nessun Paese, per quanto a conoscenza degli autori, sono state adottate norme sul reciproco riconoscimento degli atti notarili elettronici. Ma anche sotto il profilo puramente interno, hanno tardato ad emergere norme che autorizzassero la redazioni di atti in forma elettronica. In Germania l'emissione di copie conformi di documenti cartacei fu disciplinata solo nell'aprile 2006 (JKomG, http://www.egvp.de/pdf/rechtsvorschriften/JKomG.pdf).

55) Presentazione al congresso dei notai europei, Roma 2005, http://www.cnue-nouvelles.be/fr/congres-2005-en/rapports-discours/2-integrated-system-for-the-processing-of-computerised-en.doc.

56) Presentazione alla conferenza "Work on E-Juctice", Bremen 2007, http://www.bmj.bund.de/files/-/1828/Vorläufige%20Fassung%20Konferenzprogramm%20-%20Work%20on%20E-Justice.pdf.

57) Tribunale di Roma, sezione XIII, 26 marzo 2005.

58) In Italia hanno luogo circa 1.700.000 trasferimenti immobiliari ogni anno, e di questi circa cinquanta danno origine a controversie legali: un irrisorio 0.003% (Consiglio Nazionale del Notariato, *Notaio, sicurezza giuridica, sviluppo economico*, Roma, Maggio 2007).

59) *The Latin Notary: the Civil Law "title insurance*" scheda non firmata (ma: di Eliana MORANDI) nella sezione inglese del sito www.notariato.it. [Per un'illustrazione in lingua italiana del meccanismo della *title insurance si veda, della medesima Autrice, Il notaio: alternativa civilistica alla title insurance?* relazione al XLI Congresso Nazionale del Notariato, Pesaro, 18/21 settembre 2005, pure disponibile su www.notariato.it NdT].

60) Convenzione che sopprime la legalizzazione degli atti pubblici esteri, conclusa all'Aia il 5 ottobre 1961.

61) Un'organizzazione permanente che esiste sin dal 1893: http://www.hcch.net. Il sito possiede una sezione dedicata all'Apostille che contiene dettagliate informazioni intorno alla e-Apostille.

62) L'Unione Internazionale del Notariato Latino, l'organizzazione mondiale dei notai di diritto latino, o Civil Law Notaries_ www.uinl.org.

63) National Notary Association, la più importante organizzazione di notai statunitensi: www.nationalnotary.org.