

UNIVERSITA' DI PAVIA  
**COLLEGIO GHISLIERI**  
CENTRO STUDI DI INFORMATICA GIURIDICA

SEMINARIO  
**AMMINISTRAZIONE DIGITALE: PROCESSO AL "CODICE"**  
PAVIA, 20 MAGGIO 2005, AULA MAGNA DEL COLLEGIO

RELAZIONE DI UGO BECHINI, NOTARO IN GENOVA  
**IL CLUB DELLA FIRMA DIGITALE**

In questo *Processo al Codice* di oggi, vedo numerosi i candidati al ruolo di PM: non me ne vorrete se comincio dunque con l'assumere per qualche istante il ruolo dell'avvocato difensore. Il Codice recepisce infatti due punti che mi stavano particolarmente a cuore, e su cui ero già intervenuto con un articolo insieme al mio stimatissimo Amico e Collega Mario Miccoli <sup>1</sup>.

Chiamiamo firma elettronica, e più precisamente firma elettronica leggera, qualunque associazione di dati informatici ad una identità, tanto che (esempio limite) deve probabilmente considerarsi firma elettronica leggera anche un comunissimo SMS, in quanto esiste un collegamento alla identità di una persona, realizzato attraverso l'indicazione del numero del mittente. E' un collegamento labile sinché si vuole, ma pur sempre un collegamento. Se la firma elettronica leggera integra gli estremi della forma scritta, come prevede la legislazione vigente oggi, nel 2005, dobbiamo concludere che con uno scambio di SMS si può vendere un immobile: il codice civile si accontenta della forma scritta. Nel contempo la legge ci dice però che il giudice può liberamente apprezzare l'attendibilità di questa forma di documentazione sul piano probatorio. E qui la confusione è totale. La forma scritta serve anche (e forse soprattutto) per assicurare che un determinato tipo di contratto sia documentato con un elevato grado di certezza. Statuire che siamo dinanzi ad una forma scritta ma che dal punto di vista probatorio ogni giudice si regola come meglio preferisce (questo in definitiva dice la legge) significa fare a pezzi la coerenza del sistema. Mi pare dunque un sostanziale passo in avanti l'eliminazione di quella previsione: la firma leggera non integra più gli estremi della forma scritta.

Il Codice compie un'altra operazione che vedo col massimo favore: anche in caso di firma digitale propriamente detta, la provenienza del documento dalla persona che risulta titolare del certificato di firma diviene suscettibile di prova contraria. Il problema di fondo, qui, consiste nel fatto che la firma digitale è qualcosa di intrinsecamente diverso dalla firma cartacea. Magari con qualche incertezza, ma tendenzialmente si può sempre dimostrare quale persona fisica ha apposto una determinata sottoscrizione tradizionale su carta: ci sono i periti calligrafi per questo. La firma digitale invece, almeno fino a quando non si

introdurranno e renderanno obbligatori in qualche forma ausili di tipo biometrico, documenta soltanto che una determinata firma è stata apposta utilizzando una determinata smartcard, che come è noto consiste semplicemente in una tesserina delle dimensioni di un bancomat. Manca qualunque indizio sull'identità della persona fisica che ha apposto la firma.

La legislazione italiana sin dal 1997 aveva preso una direzione a suo modo netta: ignorava il problema. Chi decideva di dotarsi di firma digitale si assumeva contestualmente tutti i rischi connessi all'utilizzo di questo strumento. Qualunque documento sottoscritto con la firma digitale di Tizio gli sarebbe stato imputabile *tout court*, restando irrilevante il fatto che davvero il documento fosse stato sottoscritto dal titolare.

Questo tipo di approccio è criticabile almeno su due fronti.

La logica secondo cui chi sceglie un mezzo di comunicazione è responsabile del suo cattivo funzionamento è principio sacrosanto in diritto privato e ancor più nel diritto commerciale (la giurisprudenza in materia di telegrafo risale all'epoca dei nostri bisnonni, probabilmente ...) ma fatto è che la legge o le fonti subordinate impongono talora l'uso della firma digitale, per esempio alla presentazione dei bilanci delle società. Porre a carico di un soggetto la disfunzione di un sistema che non ha scelto, ma che al contrario gli è stato imposto, è una soluzione in palese conflitto con i principi.

Oltre al richiamato problema della mancanza di un collegamento fisico, vi sono altri profili che rendono un po' complicato attribuire *tout court* ad un soggetto un atto firmato digitalmente. Gli americani dicono *Granma chooses the wrong password and loses her house* cioè *la nonna sceglie la password sbagliata e perde casa sua*: è abbastanza facile firmare digitalmente un documento per un altro. Potete credere ad un notaio ruspante come me che deve mettere alcune migliaia di firme digitali ogni anno: quello di firmare un documento per un altro è un serio rischio da cui ci dobbiamo continuamente guardare. Si aggiunga poi che il sistema di firma è ragionevolmente sicuro in sé, ma attaccabile indirettamente in molti modi, non ultimi i virus.

Vi è infine una questione più sottile, quella della riconoscibilità sociale del gesto. Immaginiamo che io voglia contestare un prelievo Bancomat, sostenendo che non avevo inteso che recandomi ad uno sportello automatico ed usando la mia carta ed il mio PIN avrei prodotto un addebito sul mio conto corrente: sarei poco credibile, per evidenti motivi. Se invece, manovrando un software, firmo il file *alifyu.pdf* che poi scopro essere un'alienazione immobiliare, andare davanti un giudice e dire che non avevo compreso che premendo quei tasti sul PC avrei venduto casa mia, è decisamente più plausibile.

Questo è d'altra parte l'orientamento internazionale più diffuso, soprattutto nei paesi anglosassoni.

Stephen Mason, che è forse lo studioso più accreditato di firma digitale in Inghilterra, autore di un importante volume apparso nel 2003, afferma molto chiaramente che la firma digitale non rappresenta prova della provenienza di un documento da un soggetto: la prova deve essere fornita altrimenti, di per sé la firma digitale non lo prova. In termini anche più crudi afferma la stessa cosa la giurista statunitense più autorevole in materia,

Jane Winn, la quale ha sempre sostenuto con franchezza tutta texana che la firma digitale non prova l'identità di chi ha firmato un documento.

Io da qui però vorrei allargare il discorso. Nei sacri testi in tema di firma digitale, l'esempio classico è quello di Alice e Bob: Alice deve mandare un documento a Bob e viene spiegato come il meccanismo della firma digitale consenta a Bob di rendersi conto che questo documento proviene effettivamente da Alice.

Il problema è che nelle applicazioni pratiche (sino ad oggi, almeno) abbiamo visto che ben difficilmente siamo di fronte a documenti che vanno da Alice a Bob: si tratta quasi sempre di documenti inseriti in un più ampio sistema. Desidero mostrarvi alcune slides che mostrano quello che abitualmente fanno i notai in Italia [*infra, figure da 1 a 3*]. Dopo aver ricevuto una vendita d'immobile, il notaio prepara un file xml, cioè un file in cui, oltre al testo dell'atto, tutte le informazioni rilevanti contenute nell'atto sono taggate, cioè inserite all'interno di campi rigidamente prestabiliti (una sorta di modulo): in tal modo è assai semplice realizzare softwares che vanno automaticamente a recuperare all'interno del file XML i dati che di volta in volta interessano.

L'applicazione pratica che noi notai ne facciamo, nota come *Adempimento Unico*, è concettualmente semplice ma davvero molto funzionale. Stipulata la nostra compravendita, mandiamo un solo file ad un ufficio pubblico, che in questo caso è il Ministero delle Finanze. Non tutti i dati interessano a tutte le amministrazioni. Ad esempio il Comune, ai fini dell'aggiornamento dell'archivio degli immobili a fini ICI, ha interesse a sapere chi è il proprietario dell'immobile, ma non a conoscerne altri elementi, come il prezzo pagato, che invece interessa (e molto!) all'Amministrazione Finanziaria. L'amministrazione che riceve per prima il file funge da capofila: apre il file xml inviando in via automatizzata alle altre amministrazioni i dati che a ciascuna interessano.

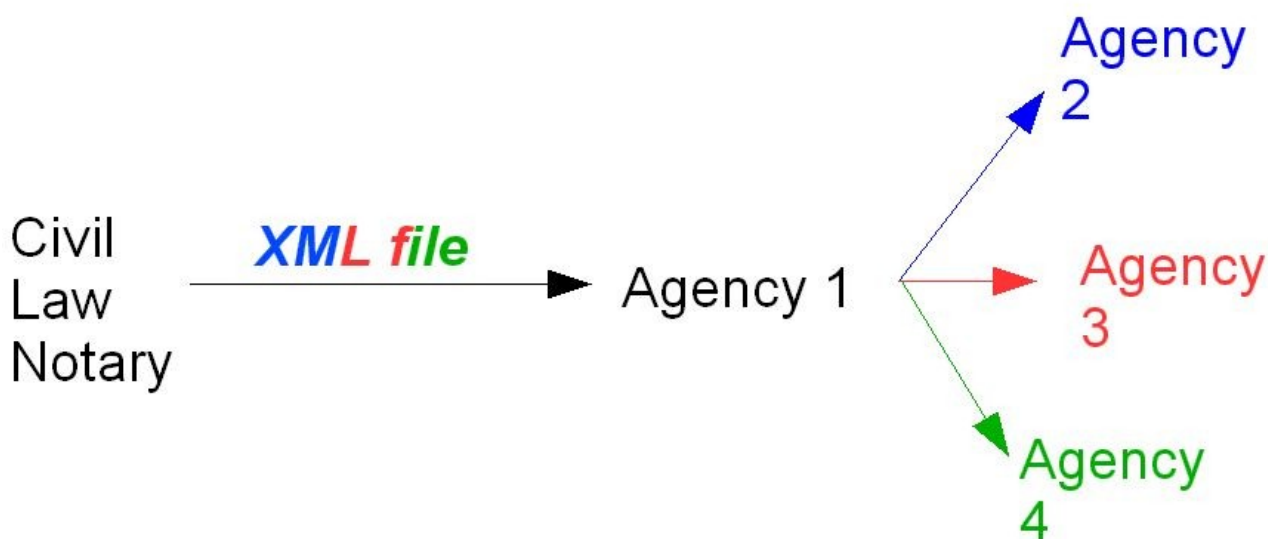
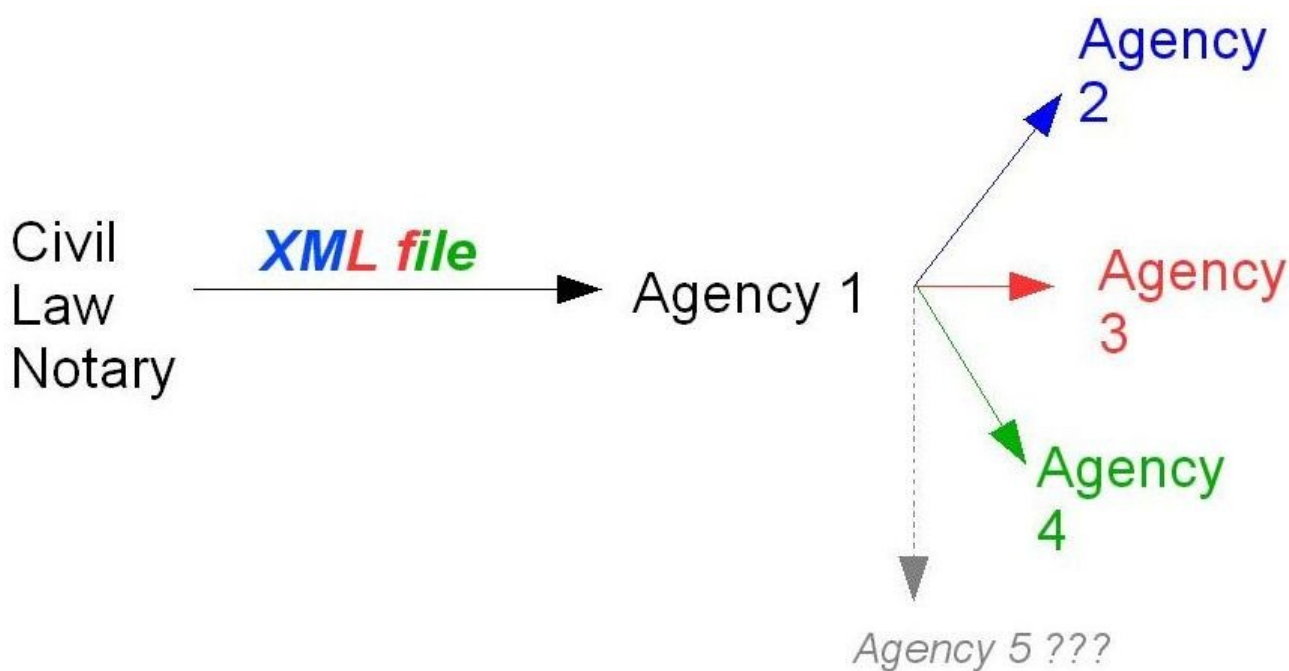


Fig. 1. Il file XML, contenente tutti i dati relativi all'operazione, viene trasmesso ad un unico Pubblico Ufficio, che si occupa di "spacchettare" l'insieme e di trasmettere ad ogni ufficio interessato i diversi dati (simboleggiati con i diversi colori) che a ciascuno occorrono

Il fatto che la procedura sia automatizzata ed informatizzata annulla anche le complicazioni logistiche, che nel mondo cartaceo sono notevoli: se un notaio di Palermo riceve un atto relativo ad un immobile sito a Portofino, i dati per la registrazione devono essere inviati all'Ufficio Entrate di Palermo, che è competente a riscuotere le imposte di trasferimento, ma l'aggiornamento catastale sarà da presentarsi al catasto di Genova, che è competente per Portofino, mentre i registri immobiliari sono a Chiavari, il Comune è evidentemente Portofino e così via.

Stiamo parlando quindi di un sistema che interessa già d'ora diverse centinaia di uffici, e potenzialmente, considerando tutti i Comuni, qualche migliaio. Quel che è più interessante, qualunque allargamento si voglia pensare ad altri Uffici ed altre Amministrazioni, non occorrerà modificare né il file XML né la tecnica di invio: è sufficiente che l'ufficio capofila istruisca le sue macchine nel senso di eseguire un'altra copia dei dati da mandare alla nuova Amministrazione.



*Fig. 2. Qualora una nuova amministrazione (Agency 5) entri a far parte del sistema, nulla muta nell'adempimento a carico dell'utilizzatore del sistema*

Non sto parlando di un progetto, ma di una cosa che si sta concretamente praticando in tutta Italia mentre si svolge questo convegno. Ed anzi il sistema attualmente in funzione è più complesso di così. Il file che viene mandato dal notaio contiene i dati del conto corrente del notaio. La ragione è semplice. Il cliente paga le imposte al notaio che le versa in banca su un suo conto corrente apposito, che in gergo si chiama (confesso di non saperne dire il perché) conto gabbietta. Il file xml contiene tutti i dati e l'ordine alla banca di pagare, il Ministero delle Finanze manda quest'ordine alla banca del notaio, aspetta la

risposta e dopo di che il tutto prosegue. E' un'aggiunta importante: il pagamento di imposte anche per importi molto rilevanti, che passano in maniera del tutto automatizzata.

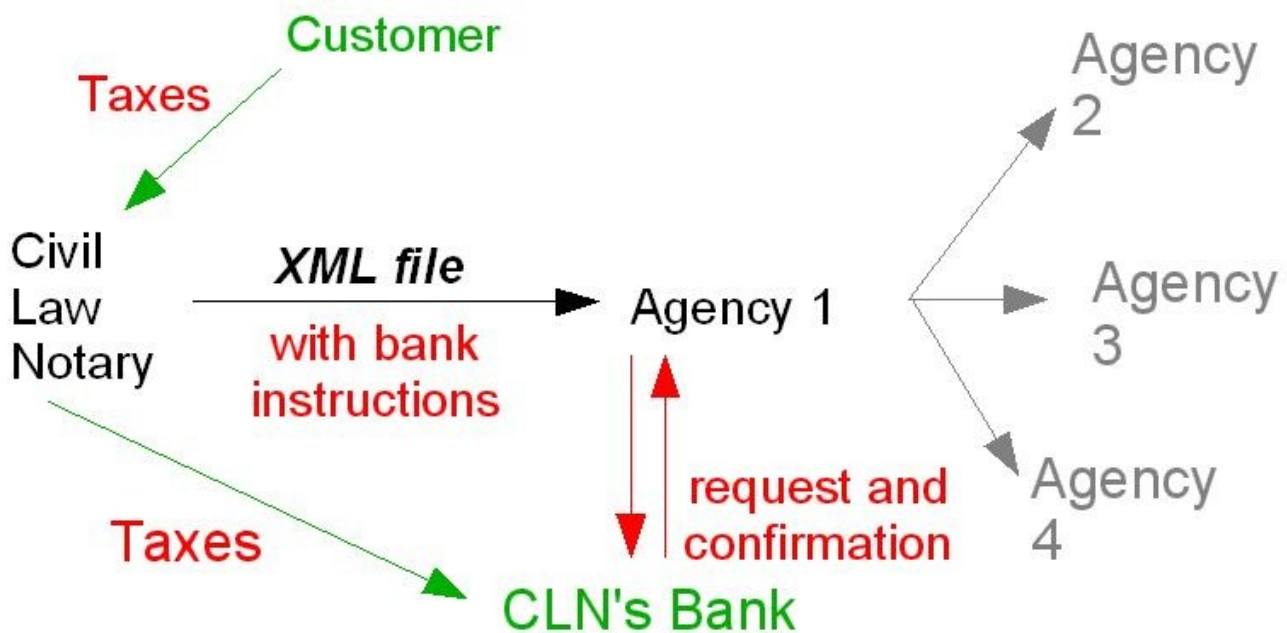


Fig. 3. Le frecce verdi indicano il percorso seguito materialmente dal denaro occorrente per il soddisfacimento delle imposte: dal cliente al notaio alla banca. Il file XML contiene anche le istruzioni bancarie, ed il pagamento alle Amministrazioni ha dunque luogo senza alcun intervento manuale

Sistemi di questo genere presuppongono un'organizzazione non trascurabile. Un esempio. Attualmente non è possibile eseguire per via telematica la trascrizione dell'atto ai registri immobiliari. Il motivo è interessante: dato che ai registri immobiliari non accedono solo gli atti notarili, ma anche altri documenti, come i sequestri o i pignoramenti ordinati dal giudice, come si fa a passare al telematico visto che non tutti i Tribunali d'Italia sono pronti ad emettere copia dei loro documenti in forma digitale?

Si può pensare ad un sistema dove convivano formalità cartacee e formalità elettroniche, ma subito è apparso chiaro un problema. Immaginiamo che qualcuno, appreso che a mezzogiorno è stato emesso il provvedimento di pignoramento di casa sua, si precipiti dal notaio a vendere l'immobile. Se il notaio trascrive subito si rischia che alle otto del mattino successivo, quando l'avvocato si presenta in Conservatoria con il "suo" pignoramento, l'immobile sia già passato di mano. Né l'avvocato potrebbe farci alcunché, atteso che a mezzogiorno lo sportello fisico chiude. Bisognerebbe inventare un sistema che accodi, come suol dirsi, documenti informatici e cartacei, che cioè garantisca che la sequenza di trattamento rispetti la priorità di presentazione. Non in tutte le applicazioni l'accodamento è vitale ma nei registri immobiliari lo è.

In Québec hanno risolto questo problema in maniera molto netta: chi ha il documento cartaceo deve rivolgersi ad un certo ufficio pubblico che, con tutta la calma del caso, scannerizza il documento e vi applica una firma digitale: in questo modo il documento passa sicuramente indietro a tutti gli altri e ne deriva ovviamente una forte pressione a passare al digitale.

Ho voluto dedicare qualche istante alla descrizione del sistema notarile per trarne un insegnamento di portata più generale. Sistemi come questi sono circuiti chiusi in cui non è, almeno in prima battuta, rilevante l'identità di chi trasmette, quanto il suo status. Alla Conservatoria dei Registri Immobiliari poco importa che sia Alice o Bob ad aver firmato l'atto: quel che davvero conta è si tratti di un notaio regolarmente in esercizio.

Nel nostro sistema, in effetti, non è strategico che il file XML venga da un notaio piuttosto che da un altro. Si controlla soltanto che la firma sia apposta in applicazione di un certificato emesso dal Consiglio Nazionale del Notariato, il quale a sua volta rilascia sistemi di firma solo ai notai in esercizio, e si preoccupa anche di revocare alla svelta il certificato laddove il notaio cessi per qualunque causa dalle sue funzioni.

In definitiva è solo questo che interessa controllare: che la firma appartenga ad UN notaio, UN commercialista, UN avvocato. Chi sia la persona si può controllare naturalmente in caso di contestazione, ma non è quello il cuore del sistema. Assistiamo insomma oggi allo svilupparsi e al diffondersi della firma digitale nell'ambito di club professionali chiusi che dedicano delle risorse importanti alla costruzione di sistemi di questo tipo, che posseggono aspetti di una certa complessità.

Un esempio. Appena una settimana fa il sistema notarile che vi ho descritto è rimasto bloccato per una lunghissima mezza giornata. Era accaduto che la lista dei certificati revocati non fosse stata scaricata correttamente dal Ministero delle Finanze. Quando si verifica una firma, si controlla anche che il relativo certificato non sia stato revocato, per essere certi, tra l'altro, che quel notaio sia ancora nella pienezza delle funzioni. Esiste una lista dei certificati revocati che si chiama CRL, Certificate Revocation List, che viene aggiornata ogni sei ore. La lista ha una validità di ventiquattr'ore: sulla carta, se il sistema si ferma, ci sono almeno diciotto ore di tempo per rimediare. Sulla carta, per l'appunto. Per qualche motivo il server che doveva produrre questa lista si pianta nel bel mezzo di un weekend. I sistemi di allerta, per qualche altra diabolica ragione, non scattano. Al lunedì mattina tutti i notai d'Italia provano a registrare i loro atti ma vengono tutti respinti: in mancanza di una lista dei certificati validi il sistema, per sicurezza, va in blocco. Il tutto per un banalissimo problema di trasmissione della lista tra un server e un altro; è stato sufficiente questo per mandare in tilt migliaia di firme digitali e di trasmissioni di questo tipo.

E questo è solo un aspetto. Chi vuole servirsi della firma digitale deve munirsi di appositi lettori di smart card e di appositi software. Ragionevolmente occorre un'installazione di riserva su una seconda macchina; il tutto richiede regolare manutenzione e deve essere ben protetto da virus, intrusioni ed altri attacchi, che potrebbero avere conseguenze disastrose. Sono dunque sistemi complessi, e francamente al momento mi sembra difficile che possano essere funzionali anche a chi debba firmare documenti solo

occasionalmente; sistemi utilizzati professionalmente per grandi quantità di documenti, dove risparmi e semplificazioni divengono significativi, sono invece decisamente appetibili.

Ecco dunque completato lo scenario cui alludevo nel titolo del mio intervento. La mia sensazione è che per il futuro prevedibile la firma digitale rimarrà un prodotto riservato ad utenti che condividono una medesima qualifica ed utilizzato per una precisa finalità.

Ma attenzione: quando parlo di club non sto necessariamente parlando di un club ristretto, nel senso di poche decine o poche centinaia di persone. Le persone che condividono una stessa qualifica possono costituire aggregati anche di enormi dimensioni. Ad esempio tutti gli elettori di un certo territorio! Così come il Consiglio Nazionale del Notariato rilascia i suoi certificati ai notai, posso ben immaginare che il Comune rilasci un certificato digitale agli elettori. C'è una differenza quantitativa, ma non qualitativa: chi è competente a stabilire chi è elettore e chi no, lo fa in forma digitale così come lo ha fatto finora in forma cartacea.

Anni fa si ragionava diversamente. Si immaginava che ognuno avrebbe avuto una sola smart card, con la quale avrebbe fatto tutto, magari integrata dai cosiddetti certificati di attributo.

Oggi mi pare che il trend si sia ribaltato, e si tenda a rilasciare un certificato di firma per ogni club di cui l'utente fa parte, finalizzato ad un uso ben preciso. Ogni Ente od Amministrazione può così identificare i suoi interlocutori senza dipendere da certificazioni operati da altri soggetti: può rilasciare e revocare i certificati in piena autonomia; la revoca o scadenza di un certificato non incide su nessun altro rapporto. <sup>ii</sup>

Al momento, a quanto sembra, non abbiamo dunque l'identità digitale, ma **le** identità digitali. Non è poi detto che sia un passo indietro.

Grazie a tutti voi per l'attenzione!

i

□

Ugo BECHINI e Mario MICCOLI, Attuazione della direttiva europea sulla firma elettronica, ovvero la forma sine probatione (commento al d.leg. 23 gennaio 2002 n. 10), in *Notariato (IPSOA)*, 2002, p. 324.

ii

In un contributo apparso alcuni mesi dopo questo intervento (*Fighting Fat-Wallet Syndrome*, in *Wired News*, 9 febbraio 2006), il celebre specialista statunitense Bruce Schneier individua questa tra le ragioni dell'inesorabile moltiplicazione delle carte di credito e fidelizzazione nei portafogli degli americani, fenomeno che parrebbe a prima vista facilmente evitabile: *Everyone has different rules for card issuance, expiration and revocation, and everyone wants to be in control of their own cards. If you lose control, you lose security.* Un'ulteriore causa individuata da Schneier per questa proliferazione è il cosiddetto *branding*: ogni operatore commerciale, per ragioni di visibilità presso il consumatore, preferisce distribuire una carta con il proprio logo. Questo argomento sembrerebbe inapplicabile al mondo della Pubblica Amministrazione, ma non è affatto detto (anzi!) che l'elemento prestigio non abbia una sua importanza anche in tale contesto.