Aspetti giuridici delle smart card come strumenti di firma e di pagamento

di Massimo Farina

L'uso delle smart card è largamente diffuso, in quanto rappresentano uno strumento in grado di fornire validità ed efficacia giuridiche alle operazioni compiute, per il tramite di Internet, fra soggetti distanti. Non solo, oggi la smart card è in grado di sostituire la moneta contante e tutti i suoi surrogati e di conseguenza diviene uno strumento di pagamento valido per l'estinzione dei debiti pecuniari. Tutto ciò investe aspetti tecnici ed, inevitabilmente, giuridici.
L'uso di massa di tale tecnologia, infatti, impone un corretto inquadramento dal punto di vista giuridico del valore da attribuire alle operazioni effettuate. La moneta elettronica, la firma digitale e la carta di identità elettronica, per nominarne soltanto alcuni, sono chiari esempi del connubio tra diritto e nuove tecnologie.
Si analizzeranno, di seguito, alcuni aspetti legati all'uso delle smart card come strumento per la Firma Digitale e come mezzo di pagamento alternativo alla moneta tradizionale, con particolare riferimento agli aspetti giuridici.

Dispositivo di Firma e ruolo dei certificatori

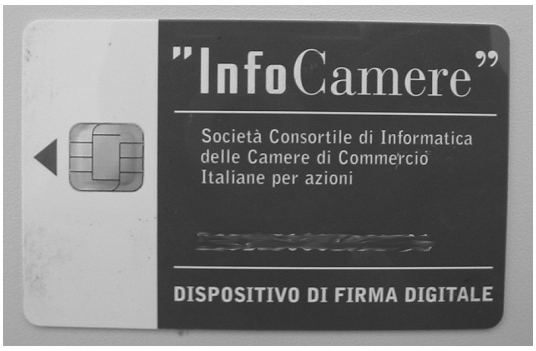
Il 1 gennaio del 2006 entra in vigore il Decreto legislativo n. 82 del 7 marzo 2005 recante il "Codice dell'Amministrazione Digitale". Il suddetto Decreto si sostituisce, così com'è disposto dal suo articolo 76, al T.U. 445/2000, meglio conosciuto con il nome di "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" (o T.U.D.A.). Le vicende delle firme elettroniche sono, però, tutt'altro che concluse. Si assiste, in questi giorni, all'elaborazione di nuove regole, che dovrebbero integrare il Codice dell'Amministrazione Digitale, dai contenuti molto discussi e di cui si tratterà brevemente di seguito. In uno scenario così altalenante rimane fermo e quasi insensibile alle modifiche vissute dal 1997 ad oggi il riferimento allo strumento necessario per apporre una firma digitale: la *Smart Card* (**Figura 1**). Si tratta del cosiddetto "*dispositivo di firma*", così denominato dal legislatore nel pieno rispetto del principio di neutralità; il diritto positivo, infatti, non deve rallentare lo sviluppo tecnologico.

Se è vero che oggi il concetto di firma digitale è esclusivamente identificato con la *smart card*, ossia un tesserino delle dimensioni di una carta di credito, provvisto di un microprocessore e di una certa quantità di memoria, è altrettanto vero che il dispositivo di firma potrebbe essere anche una *cryptobox*, cioè una "scatola" da collegare all'esterno del computer che provvede alla cifratura e decifratura delle informazioni contenute, oppure carte a microprocessore la cui funzione principale è diversa, come ad esempio le **carte d'identità elettroniche**. Per fare in modo che il dispositivo di firma sia davvero sicuro, all'atto della fabbricazione o dell'inizializzazione devono essere inserite delle informazioni successivamente immodificabili. Tutto ciò può essere ottenuto, per esempio, attraverso la distruzione dei circuiti che consentono la scrittura in specifiche aree di memoria; diventa, così, assolutamente impossibile modificare i valori contenuti nelle aree interessate. Un *floppy disk* non potrebbe mai diventare un dispositivo di firma in quanto esso è facilmente riproducibile ed, inoltre, non può essere programmato esclusivamente all'origine. Fin dal 1999, con il primo regolamento tecnico dedicato alla Firma Digitale, si identificava il dispositivo di firma con la Smart Card. Tutt'ora, il programma informatico adeguatamente configurato (software) o l'apparato strumentale (hardware), usati per la creazione della firma elettronica, sono concretamente materializzati in una *Smart Card*; dotata di un microprocessore contenente un codice segreto che al suo interno racchiude un dispositivo di firma sicuro rilasciato da un **Ente Certificatore**.

Massimo Farina mfarina@infomedia.it

È Patrocinatore Legale del Foro di Cagliari. È specializzato in Informatica Giuridica e lavora come consulente freelance nell'ambito della formazione e dei servizi alle Pubbliche Amministrazioni ed alle imprese.

FIGURA 1 La smart card rilasciata da Infocamere



Il titolare, al quale è stata rilasciata la Smart Card, può apporre la propria firma digitale su un qualsiasi documento elettronico. Il risultato ottenuto attraverso l'operazione di firma conserva informazioni riguardanti il soggetto sottoscrittore e, nel contempo, il testo sottoscritto.

La tecnologia adottata per la firma digitale è in grado di garantire l'autenticità, cioè l'identificazione certa del soggetto che lo ha creato o spedito; l'integrità, ossia la sicurezza che il contenuto sia genuino (in caso di alterazione del documento firmato, l'operazione di decifratura con la chiave pubblica darebbe esito negativo); la certezza temporale riferita al momento di apposizione della "marca temporale"; la non ripudiabilità del contenuto, infatti il sottoscrittore non può negare di aver formato o spedito il documento.

Chiunque volesse dotarsi di un sistema di firma digitale deve rivolgersi ad un Ente Certificatore e farne apposita richiesta, nonché dotarsi del software e dell'hardware necessario.

Il Certificatore, o **terza parte fidata**, ha la funzione di garantire l'identità degli utenti che interagiscono nel web; essi attestano la corrispondenza tra persona fisica, o giuridica, e chiave pubblica da essa usata. Il certificato è costituito da un file in **standard X.509** contenente le seguenti informazioni: numero di serie o altro codice identificativo del certificato; dati identificativi del Certificatore emittente; dati identificativi dell'utente titolare di firma; dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare; **periodo di validità** del certificato medesimo; eventuali informazioni non necessarie, quali, ad esempio "le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza". Merita una breve precisazione il riferimento al periodo di validità. I certificati, infatti, sono da considerare alla stessa stregua dei documenti identificativi e come questi hanno una scadenza (biennale); è preciso compito del certificatore emittente provvedere alla revoca, verifica e sostituzione dei certificati. L'attuale impianto normativo prevede l'esistenza di tre distinte categorie di certificatori: i certificatori (in generale), i certificatori qualificati e i certificatori accreditati presso il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione); quest'ultimo è il livello più alto di certificazione. Dal 2002, con Decreto Legislativo n. 10 l'attività di certificazione è stata liberalizzata. Oggi, ai sensi dell'articolo 26 del "Codice dell'Amministrazione Digitale", non è più necessario chiedere l'autorizzazione preventiva per esercitare attività di certificazione. La disciplina in esame richiede, come unica condizione, il possesso dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche [1]. L'accertamento successivo dell'assenza o del venir meno di tali requisiti comporta il divieto di prosecuzione dell'attività intrapresa. L'ente preposto al controllo dei requisiti richiesti dal codice è il CNIPA che procede d'ufficio o su segnalazione motivata di soggetti pubblici o privati e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti.

Il successivo articolo 27 precisa che per il rilascio di certificati qualificati sono necessarie ulteriori condizioni che garantiscano maggiore affidabilità e sicurezza. I certificatori qualificati hanno l'obbligo di comunicare l'inizio dell'attività di certificazione al CNIPA con allegata una dichiarazione attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice. Tale comunicazione può essere effettuata anche per via telematica. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, devono presentare apposita richiesta di accreditamento presso il CNIPA. La certificazione proveniente da un certificatore, appartenente a ciascuna delle tre categorie sopra indicate, presenta diversi gradi di sicurezza. Talvolta è richiesto che la firma elettronica sia autenticata da un certificatore appartenente a una specifica categoria; ad esempio, il documento informatico ha l'efficacia prevista per la scrittura privata dall'articolo 2702 del codice civile se è sottoscritto con la firma digitale o con un altro tipo di firma elettronica qualificata [2]; in altri casi, e precisamente per la validità delle istanze e delle dichiarazioni presentate alle pubbliche amministrazioni per via telematica, è richiesta la sottoscrizione mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato [3].

Valore ed efficacia legali delle firme elettroniche nel Codice dell'Amministrazione Digitale

L'evoluzione normativa del documento elettronico e della Firma Digitale nello scenario italiano è stata

assai lunga e travagliata [4]. In principio il legislatore si dedicò esclusivamente alla Firma Digitale, originando in tal modo la triplice distinzione tra "firma forte", "firma debole o leggera" e "documento elettronico (privo di firma)". Successivamente, anche dal punto di vista normativo si è passati ad una più variegata classificazione; ciò per via del necessario adeguamento alla direttiva, 1999/93/CE, sulla firma elettronica. Infatti con il Decreto Legislativo 10/2002 si moltiplica, a livello normativo, il numero di firme elettroniche: **firma elettronica semplice, avanzata, digitale** e **qualificata**, tutte appartenenti al genere firma elettronica. Sul valore ed efficacia riconosciuti alle diverse specie di "firme elettroniche" codificate si è scritto, e discusso, tanto. Molti dei problemi sollevati in passato appaiono risolti con le nuove disposizioni contenute nel Decreto Legislativo n. 82/2005 ma arrivano già proposte correttive. Il 17 ottobre 2005, presso il Dipartimento dell'Innovazione, si è tenuta una riunione per discutere le modifiche al Codice dell'Amministrazione Digitale, finalizzata alla stesura di decreti "*integrativi e correttivi*" a norma dell'articolo 10 della Legge Delega n. 229/03. In questi giorni circola una bozza [5] del suddetto decreto correttivo che presenta modifiche aspramente criticate da Voci autorevoli [6]. In attesa di ulteriori sviluppi, anche in seguito all'approvazione di eventuali Decreti Legislativi modificativi, si tratterà, di seguito, esclusivamente di quanto attualmente disposto per gli aspetti di validità ed efficacia legali delle Firme Elettroniche.

Le fattispecie da analizzare sono le seguenti: "documento elettronico non firmato", "documento elettronico sottoscritto con firma elettronica semplice" e "documento elettronico sottoscritto con firma digitale".

Quanto al primo caso, può affermarsi l'equivalenza di tale documento alle riproduzioni meccaniche. L'articolo 23 del Decreto Legislativo n. 82/2005 dispone, infatti, un'integrazione al testo dell'articolo 2712 del Codice Civile, inserendo un chiaro riferimento alle "riproduzioni informatiche". Il semplice documento elettronico, a seguito di tale modifica, "*forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale è prodotto non ne disconosce la conformità ai fatti o alle cose medesime*". Chi desidera privarlo di efficacia probatoria ha l'onere di disconoscerlo; in caso contrario il valore sarà di piena prova.

Il documento sottoscritto con firma elettronica semplice (cosiddetta "firma debole") è liberamente valutabile in giudizio. È compito del giudice decidere quale valore attribuire a questo tipo di firma, previa valutazione delle "*caratteristiche oggettive di qualità e sicurezza*". Tale previsione ha fatto discutere parecchio [7] soprattutto riguardo alla definizione di firma elettronica: "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica*". Accade, infatti, sulla base di una lettura non tradizionale della disposizione, che ID e Password, digitati per accedere al servizio di *web-mail*, siano intesi come forma di autenticazione informatica ossia come **firma elettronica**. Una lettura più fedele al dato letterale inquadra l'*e-mail* tra i documenti informatici sprovvisti di firma elettronica il cui valore è semplicemente quello delle "*riproduzioni meccaniche*" previste all'articolo 2712 del Codice Civile.

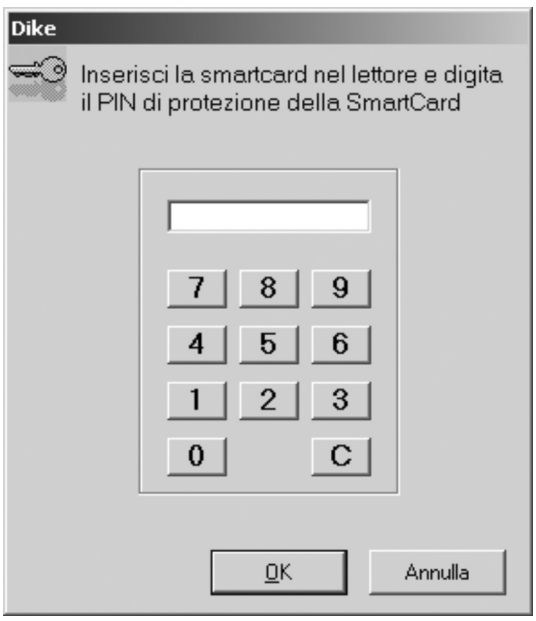
La firma digitale o altro tipo di firma elettronica qualificata, infine, sono pienamente equivalenti alla scrittura privata. L'articolo 21, comma 2, del Decreto Legislativo n. 82/2005 dispone che il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale "ha l'efficacia prevista dall'articolo 2702 del codice civile". In altri termini, "*fa piena prova […] 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*".

Come già sopra affermato, in attesa di eventuali modifiche, l'attuale comparto normativo dedicato al valore ed efficacia legali delle firme elettroniche e del documento informatico è quello poc'anzi esposto.

La Moneta elettronica

La **rivoluzione informatica** ha notevolmente modificato tempi e modalità delle transazioni commerciali. Sono molteplici gli interventi normativi, a livello nazionale e comunitario, riguardanti il commercio elettronico, spesso orientati verso la tutela del consumatore [8]. Va subito precisato che l'*e-commerce* non è soltanto scambio di proposta ed accettazione negoziale

FIGURA 2 Richiesta del PIN per apporre la firma digitale



ma, altresì, nella accezione omnicomprensiva del termine, **pagamento del prezzo**. Il mezzo tradizionale per estinguere un debito di pagamento è la moneta. Ciò è in linea con quanto affermato nell'art. 1277 del codice civile che esattamente recita: "*I debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale*".

Ebbene, nell'attuale mercato della rete i contratti hanno perso la connotazione esclusivamente empirica a favore della virtualità. Ciò vale, ovviamente, anche per la moneta. La "circolazione monetaria elettronica" consiste nella possibilità di adempiere alle obbligazioni pecuniarie (cioè ai debiti consistenti in somme di denaro) in modo non fisico. Non si realizza, infatti, la consegna materiale della moneta, tantomeno di titoli rappresentativi cartacei. I sistemi informatici permettono il trasferimento, da un soggetto ad un altro, di un flusso di dati corrispondenti, per convenzione, ad una specifica disponibilità monetaria.

La sempre più imponente diffusione dei sistemi di pagamento elettronici ha condotto verso una loro codificazione giuridica. La fonte più recente è data dall'art. 55 della legge n°39 del 01/03/2002 che in linea con le direttive comunitarie (2000/46/CE, 2000/28/CE), definisce la moneta elettronica come "*un valore monetario rappresentato da un credito nei confronti dell'emittente che sia memorizzato su un dispositivo elettronico, emesso previa ricezione di fondi di valore non inferiore al valore monetario emesso e accettato come mezzo di pagamento da soggetti diversi dall'emittente*".

La proiezione materiale della moneta elettronica è costituita dalla smart card con microprocessore in grado di accumulare dati convenzionalmente equivalenti alla moneta ed, allo stesso tempo, di compiere le operazioni matematiche necessarie a quantificare l'aumento o la diminuzione di valore. In seguito a ciascuna operazione d'acquisto il borsellino contenuto nella smart card si svuota progressivamente; viceversa, il contenuto lievita ad ogni nuova ricarica. Come avvengono, in concreto, queste operazioni di ricarica e di spesa della moneta virtuale? Il titolare della *smart card* trasferisce sul microprocessore un valore monetario pari ad un importo monetario precedentemente versato, in moneta contante, presso un ***ATM*** (*Automatic Teller Machine*) appositamente programmato per addebitare contestualmente l'importo sul conto corrente del titolare, o un istituto di credito. Effettuata la ricarica, è possibile eseguire operazioni di pagamento tramite l'inserimento della smart card nel ***POS*** (*point of sale*) dell'esercente venditore; quest'ultimo digita l'importo del pagamento e riconsegna lo strumento di pagamento al titolare. Sarà sufficiente verificare l'importo digitato e premere un tasto per far si che avvenga il trasferimento elettronico di **bit monetari**. La disponibilità patrimoniale si trasferisce immediatamente dalla carta di pagamento al *POS* del venditore. Il trasferimento del credito non viene posticipato nel tempo ma è istantaneo, come se si trattasse di trasferimento di monete o di banconote. Il ruolo dell''ente creditizio è preliminare all'operazione di trasferimento di fondi. Egli provvede a dotare i soggetti interessati dello strumento di moneta elettronica. Durante la transazione il rapporto intercorre esclusivamente tra debitore e creditore; essi trasferiscono delle disponibilità monetarie senza necessità di alcun intervento esterno che assicuri la bontà del pagamento. Manca la fase del cosiddetto **buon fine** dell'operazione. Il "denaro" che transita dalla *smart card* al *POS* è concretamente costituito da impulsi elettronici che verranno successivamente convertiti in qualsiasi valuta ed al corso di cambio vigente al momento del trasferimento. Il rapporto intercorrente tra il titolare della smart card e l'istituto emittente è totalmente regolato dalle parti; si tratta di una disciplina di natura esclusivamente convenzionale; restano fermi gli obblighi previsti per i fornitori di servizi di moneta elettronica verso i consumatori e cioè: informazione, trasparenza e rimborsabilità su richiesta del titolare della carta per tutto il periodo di validità della stessa.

Le transazioni descritte avvengono in modalità *off-line*; ciò le distingue dai tradizionali mezzi di pagamento elettronici, come i bancomat o le carte di credito. La moneta elettronica non necessità, infatti, della linea telefonica, di conseguenza il venditore non sopporta costi di connessione per ciascuna operazione di compravendita; egli spenderà una sola volta per il trasferimento della disponibilità monetaria dal *POS* al proprio conto corrente. Inoltre, il trasferimento *off-line* garantisce una maggiore sicurezza nelle transazioni, le quali non sono soggette alle insidie tipiche delle reti. L'utilizzo della moneta elettronica garantisce sicurezza anche dal punto di vista del cosiddetto **rischio monetario**, tipico delle operazione effettuate con modalità *EFT* (*Electronic Funds Transfer*).

L'importo caricato sul microprocessore della smart card è, di regola, limitato, spesso sufficiente per una sola operazione di acquisto. Si pensi, al contrario, alla carta di credito che, se inserita nel circuito, può essere utilizzata in modo fraudolento per l'intero *plafond* mensile disponibile; questo è un rischio assai maggiore rispetto a quello che si corre in caso di perdita del **prepagato**, di ammontare irrisorio.

A quanto detto si aggiunga la non necessità di un software di cifratura, l'anonimato del titolare del microprocessore ed il trasferimento del flusso monetario contestualmente al compimento dell'operazione. Sono tutti validissimi motivi per affermare la sicurezza di questo strumento di pagamento rispetto agli altri surrogati monetari di natura tecnologica. Da quanto fin qui esposto pare potersi affermare che la moneta elettronica si presta, in modo esclusivo, per le transazioni di piccolo importo, replicando le funzioni tipiche del titolo al portatore (la banconota o la moneta).

Bibliografia

[1] Decreto Legislativo 1° settembre 1993, n. 385, e successive modificazioni.

[2] Articolo 21, comma 2, Decreto Legislativo n. 82 del 7 marzo 2005 recante il Codice dell'amministrazione digitale.
[3] Articolo 65, comma 1, lettera a), Decreto Legislativo n. 82 del 7 marzo 2005 recante il Codice dell'amministrazione digitale.
[4] M. Farina *"I sistemi di firma digitale basati su Smart card: la normativa italiana"*, DEV 121, Gruppo Editoriale Infomedia, 2004.
[5] (Bozza di) Decreto legislativo recante modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, a norma dell'articolo 10 della legge delega 29 luglio 2003, n. 229, in InterLex, http://www.interlex.it/docdigit/mod_integr.htm.
[6] M. Cammarata, Idee sempre più confuse sulle firme elettroniche, in InterLex, http://www.interlex.it/docdigit/confuse.htm
[7] M. Farina *"Riflessioni sul valore legale dell'e-mail a seguito a seguito della pronuncia di alcuni decreti ingiuntivi basati esclusivamente sulla produzione di una e-mail"*, in pubblicazione in Rassegna di Diritto Civile n.3/2005, Edizioni Scientifiche Italiane.
[8] Le principali fonti, italiane e comunitarie, in tema di commercio elettronico sono, in ordine cronologico:

- Decreto legislativo 15 gennaio 1992, n. 50
- Attuazione della direttiva n. 85/577/CEE in materia di contratti negoziati fuori dei locali commerciali;
- Decreto legislativo 31 marzo 1998, n. 114 (art. 18) - Riforma della disciplina relativa al settore del commercio, a norma dell'articolo 4, comma 4, della legge 15 marzo 1997;
- Decreto legislativo 22 maggio 1999, n. 185 - Attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza;
- Circolare n. 3487/C del 01.06.2000 "Disciplina della vendita di beni tramite mezzo elettronico" del Ministero dell'industria, commercio e artigianato sul decreto legislativo 114/88
- Decreto legislativo 9 aprile 2003, n. 70 - Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.