ATTI INFORMATICI

IL DOSSIER DEL LUNEDÌ

Il Sole 24 ORE

Lunedì 8 ottobre 2007 - **www.ilsole24ore.com**

Gli strumenti. I modelli di sottoscrizione, chi li deve rilasciare e certificare. **Pag. 38**

Le categorie. Gli utilizzatori: imprese, uffici pubblici e professionisti. **Pag. 39**

La sicurezza. Le garanzie, i rischi, i reati e le sanzioni. **Pag. 40**

Dal Sole 24 ORE

LA GUIDA OPERATIVA

FALLIMENTO

Tutti i chiarimenti al Decreto Correttivo

COSA CAMBIA CON LE NUOVE MODIFICHE

LE SCHEDE PRATICHE PER CAPIRE MEGLIO

CHIEDI IN EDICOLA LA GUIDA OPERATIVA 'FALLIMENTO'

CON 'IL SOLE 24 ORE' A SOLI 6,00€ IN PIÙ

* Offerta valida in Italia dall'8/10/2007 all'8/11/2007

Il Sole 24 ORE

www.ilsole24ore.com

Tecnologia per pochi. Prevista dieci anni fa, viene utilizzata in prevalenza da pubblica amministrazione e imprese

Firma elettronica ancora d'élite

Il documento siglato in modalità digitale equivale a una scrittura privata

Paolo Subioli

Quando il Comune di Bologna, nel settembre del 1998, rese disponibile ai propri cittadini il servizio di firma digitale, che avrebbe consentito loro di farsi riconoscere in rete in maniera sicura, oltre che di sottoscrivere documenti elettronici con piena validità legale, dimostrò per l'ennesima volta la sua capacità unica di offrire alla città servizi d'avanguardia. Dei 152 certificati richiesti nel corso della prima settimana, però, ne furono emessi realmente solo 54, e appena uno di essi fu utilizzato.

Ci fu una certa delusione, tra gli entusiasti delle "magnifiche sorti e progressive" che venivano prospettate, da un lato, dall'avvento di Internet e, dall'altro, dalle riforme anti-burocrazia del ministro Franco Bassanini. Ma le cose, dati i tempi ancora non abbastanza maturi, probabilmente non potevano andare che in quel modo.

Tutto era nato l'anno prima. Portava, infatti, la firma di Bassanini la legge 59 del 1997 che riconosceva piena validità legale ai documenti elettronici, mentre la firma digitale vera e propria veniva riconosciuta e disciplinata col successivo Dpr 513/1997, per approdare poi nel Dpr 445 del 2000 (Testo unico sulla documentazione amministrativa). La normativa era stata concepita sulla base di un criterio di analogia tra documento cartaceo ed elettronico per quanto riguarda l'efficacia probatoria, ossia il valore dei vari tipi di sottoscrizione come eventuale prove in tribunale.

La firma digitale equivaleva alla scrittura privata, mentre gli altri tipi di riconoscimento (e-mail, password) avevano un valore inferiore, simile al fax o alla fotocopia. Il Dpr 445 è stato poi modificato a più riprese, per conformare la disciplina italiana alla normativa comunitaria contenuta nella direttiva 99/93 in materia di firme elettroniche. Il provvedimento comunitario, considerando soprattutto le esigenze dell'e-commerce, era improntata a un approccio decisamente più liberista, il quale considerava accettabile anche le firme elettroniche "leggere", basate sulla semplice password, che erano alla base di successi commerciali come Amazon.com o eBay.

Oggi la legge che disciplina la firma elettronica è il Codice dell'amministrazione digitale, per il quale un documento sottoscritto con firma digitale – che è un tipo particolare di firma elettronica (si veda la pagina seguente) e che, di fatto, è l'unica diffusa qui da noi – si presume riconducibile al titolare, salvo che questi dia prova contraria. Con il Codice il documento elettronico si trasforma da opportunità in obbligo, almeno per le amministrazioni pubbliche, e quindi strumenti come la firma digitale potrebbero addirittura diventare di uso comune, man mano che le procedure elettroniche si sostituiranno a quelle tradizionali.

Il Codice prevede addirittura che, dal prossimo 31 dicembre, l'accesso ai servizi on line degli enti pubblici sia consentito solo tramite la carta d'identità elettronica o la carta nazionale dei servizi, due strumenti di autenticazione "forte" che però non sono mai decollati. Si presume che il legislatore ponga rimedio in tempo a tale errore di valutazione, che farebbe venire meno la disponibilità di molti utili servizi degli enti pubblici.

La firma digitale è dunque la tecnologia che dovrebbe consentire di effettuare qualsiasi transazione a distanza, al limite anche l'atto di acquisto di una casa. In realtà, le cose non sono così semplici, perché si tratta di una tecnologia che richiede all'utente uno sforzo particolare – dotarsi di un certo dispositivo e installarlo, curarne la custodia, pagare gli oneri, rinnovarlo – specialmente se confrontato a quanto offre oggi la Rete, dove già si possono effettuare acquisti di ogni tipo, e persino pagare le tasse, senza bisogno della firma digitale.

L'uso della firma digitale è infatti attualmente circoscritto a due ambiti: le imprese e la pubblica amministrazione. Le aziende sono vincolate a espletare per via telematica qualsiasi formalità col Registro delle imprese. Gli uffici pubblici hanno invece bisogno della firma digitale perché la digitalizzazione dei procedimenti amministrativi ha, tra i requisiti indispensabili, quello dell'identificazione sicura in Rete dei funzionari.

Nelle amministrazioni locali risultano, secondo i dati Istat 2006, in possesso di firma digitale il 19,5% dei Comuni (che diventa 29% in quelli con più di 60mila abitanti) e il 47% delle Province. Non è disponibile alcun dato sulla diffusione della tecnologia tra i cittadini, ma è da presumere che sia assai scarsa.

I passaggi normativi

Legge 15 marzo 1997 n. 59 (Bassanini uno)
- Stabilisce che «gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge»

Dpr 7 aprile 2003 n. 137
- Stabilisce che il documento informatico ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile

Codice dell'amministrazione digitale (Dlgs 82 del 2005)
- Si propone di assicurare che le amministrazioni adottino strumenti per rendere sempre disponibili tutte le informazioni in modalità digitale. In particolare, prevede che il documento informatico sottoscritto con firma digitale o con altro tipo di firma elettronica qualificata abbia l'efficacia prevista dall'articolo 2702 del codice civile

Dpcm 13 gennaio 2004
- Regola gli aspetti tecnici e organizzativi di chi opera con i documenti informatici e la firma digitale

Deliberazione Cnipa n. 4 del 17 febbraio 2005
- Contiene le regole per il riconoscimento e la verifica del documento informatico insieme agli standard di interoperabilità dei certificatori iscritti all'elenco pubblico

Un decennio in numeri

La diffusione dei nuovi strumenti digitali e il risparmio prodotto

3 milioni – Le smart card per la firma digitale rilasciate fino a oggi

45mila – I dispositivi di firma rilasciati fino a oggi, dalla Regione Lombardia in qualità di certificatore (Lisit)

20 – I certificatori iscritti nell'elenco pubblico tenuto dal Cnipa

3 miliardi di euro – Il risparmio che si otterrebbe trasferendo il 10% dei documenti dalla carta ai supporti digitali

2,7 milioni – Le smart card rilasciate, fino a oggi, da Infocamere: il 70% alle imprese e il 30% ai professionisti

70 milioni – I documenti sottoscritti con firma digitale dagli uffici pubblici nel 2007

260 milioni di euro – Risparmiati dalle aziende grazie all'uso della firma digitale per le comunicazioni con il Registro imprese

100-150 milioni – Le previsioni di documenti sottoscritti con la firma digitale nel 2008 dalla pubblica amministrazione

Piano in tre fasi per diminuire l'uso della carta

Maurizio Pirazzini

La firma digitale è in buona compagnia. Si può, infatti, considerare uno dei tre ingredienti fondamentali, insieme alla Pec (la posta elettronica certificata) e ai metodi alternativi di conservazione dei documenti, che dovranno portare a usare sempre meno carta.

Alla firma spetta garantire l'autenticità, la paternità e l'integrità del documento; alla Pec la trasmissione sicura; alla conservazione sostitutiva "stipare" in formato elettronico (Cd, Dvd e altri supporti idonei) atti legali e fiscali.

Se la firma digitale e la Pec sono sempre più conosciute, meno percepita è l'importanza di un sistema di conservazione sostitutiva, la cui assenza renderebbe priva di consistenza e certezza "temporale" i documenti sottoscritti con la firma digitale.

La conservazione sostitutiva

Il sistema di conservazione sostitutiva rappresenta la "cassaforte" dove poter custodire nel tempo, con pieno valore legale, tutta la documentazione (contratti, lettere, fatture, ecc.). L'impresa può organizzarsi autonomamente oppure può scegliere di delegare tale attività a operatori qualificati (deliberazione Cnipa 11 del 2004).

L'infrastruttura di conservazione riguarda sia i documenti cartacei (che dovranno essere digitalizzati tramite scanner) sia i documenti che nascono in origine in formato elettronico con l'utilizzo delle firma digitale. Il sistema è incentrato sulla figura del responsabile della conservazione, che provvede a validare e certificare i processi con l'utilizzo della propria firma digitale e della marcatura temporale, e alla gestione dei supporti e dell'intera infrastruttura software (per esempio, in relazione alla lettura dei diversi formati).

Una volta acquisiti nel sistema di conservazione, i documenti cartacei si possono distruggere, con notevoli risparmi nei costi di organizzazione degli archivi. Anche a livello fiscale i problemi di carattere normativo sono stati ormai completamente risolti dall'Agenzia delle entrate.

La pubblica amministrazione

Per la pubblica amministrazione la gestione informatizzata dei flussi documentali si impone non solo con riguardo alle disposizioni (ora trasfuse nel Codice dell'amministrazione digitale) che, già da un decennio, prevedono l'obbligo di utilizzo del sistema di protocollo informatico, ma anche dalla legge che fornisce le disposizioni di "principio" dei procedimenti amministrativi.

L'articolo 3-bis (introdotto nel 2005) della legge 241/1990 prevede che «per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati».

Inoltre il Codice ha introdotto il nuovo "diritto" – già operativo dal 2006 – per imprese e cittadini di richiedere e ottenere l'uso delle tecnologie telematiche. In attesa della realizzazione del piano presentato dal ministro della Funzione pubblica e dell'innovazione, Luigi Nicolais, approvato lo scorso mese di luglio, l'utilizzo delle nuove tecnologie va consolidato, in concreto, semplicemente tramite l'impulso per l'utilizzo degli strumenti che ormai da anni sono pienamente operativi.

LE OPPORTUNITÀ

Per riorganizzare gli archivi si ricorre anche alle e-mail certificate e ai metodi alternativi di conservazione

I nodi da affrontare

Restano ancora parecchi ostacoli. I pagamenti ad esempio. Per pagare l'imposta di bollo (o i diritti di segreteria) su una qualsiasi istanza alla pubblica amministrazione la procedure on line è di fatto inesistente. Non è previsto l'acquisto di un "bollo elettronico" al pezzo (così come si fa con la carta recandosi dal tabaccaio), ma si è costretti a prevedere il numero di atti elettronici su base annua, pagare in anticipo all'Agenzia delle entrate con modello F24, comunicare il tutto all'Agenzia e gestire il conguaglio a fine anno.

Inoltre le amministrazioni ancora non consentono - per la maggior parte - la possibilità di pagare tramite carta di credito o strumenti analoghi dai propri siti web, anche se il termine del 30 giugno 2007, previsto dal Codice per «l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, con l'uso delle tecnologie dell'informazione e della comunicazione» è già scaduto.

Regole Ue. Il quadro c'è, l'applicazione scarseggia

In Europa molti sistemi sono «isole»

Maria Adele Cerizza

L'Unione europea, con la direttiva 1999/93/Ce, ha fissato un quadro giuridico comune per la firma elettronica in tutto il territorio comunitario. La norma è diretta a creare le condizioni affinché i paesi della Ue siano in grado di sfruttare i vantaggi del commercio elettronico.

Secondo la Commissione europea, il cui ultimo monitoraggio risale a marzo 2006 e ha riguardato i 25 Stati membri, l'obiettivo non è stato del tutto raggiunto. Se da un lato la direttiva del 1999 ha introdotto un'armonizzazione delle disposizioni nazionali riguardanti la firma elettronica, dall'altro il suo utilizzo è stato di molto inferiore al previsto.

La risposta, quando ci si chiede perché il mercato delle "e-firme" non si sia sviluppato con maggiore rapidità, non è univoca. Un problema di ordine tecnico – spiegano da Bruxelles – è rappresentato dalla complessità della tecnologia Pki (infrastruttura globale a chiave pubblica). Questa tecnologia usa il cosiddetto sistema del " terzo fidato", grazie al quale le parti, senza mai essersi incontrate, sono libere di prestarsi reciproca fiducia su Internet.

Inoltre, in molte tra le applicazioni attuali i prestatori di servizi hanno mostrato poco interesse, essenzialmente per motivi di responsabilità giuridica, a consentire ai clienti di utilizzare il dispositivo di autenticazione per altri servizi. Ciò spiega probabilmente perché il mercato continua a essere dominato dal ricorso a diverse password monouso.

Altri fattori possono spiegare questa lentezza: l'assenza, nella direttiva, sia di disposizioni sui criteri per la prestazione di servizi di verifica della "e-firma" da parte del Psc (Prestatori di servizi di certificazione) all'utente finale, sia di disposizioni in materia di riconoscimento reciproco fra Psc.

Un ulteriore ostacolo all'accettazione è rappresentato dalla mancanza di interoperabilità tecnica a livello sia nazionale sia transfrorntaliero, fenomeno che ha dato luogo a molte "isole", in cui i certificati possono essere utilizzati per un'unica applicazione.

Un'altra ragione pratica della riluttanza constata in ambito Ue è che l'archiviazione di documenti firmati elettronicamente è ritenuta troppo complessa e incerta. L'obbligo imposto dalla legge consente di conservare i documenti per periodi che possono superare i 30 anni e impone il ricorso a procedure e tecnologie costose e macchinose al fine di garantire la leggibilità e la verifica su tale periodo di tempo.

Il confronto

Austria
- Tipi di firma: due, base e avanzata
- Uso della firma nel settore pubblico: non previsto
- Siti web: http://cio.gov.at/identity; http://www.signatur.rtr.at/en/index.html

Belgio
- Tipi di firma: base, avanzata e qualificata
- Uso della firma nel settore pubblico: previsto
- Siti web: http://www.ecri.be; http://www.minieco-fgov.be

Danimarca
- Tipi di firma: base, avanzata e qualificata
- Uso della firma nel settore pubblico: non previsto
- Siti web: http://www.e.gov.dk

Finlandia
- Tipi di firma: base e avanzata
- Uso della firma nel settore pubblico: previsto
- Siti web: http://www.om.fi/333.htm; http://www.ficora.fi/suomi/lomake

Francia
- Tipi di firma: base, avanzata e qualificata
- Uso della firma nel settore pubblico: non previsto
- Siti Internet: http://www.legifrance.gouv.fr; http://www.ssi.gouv.fr

Germania
- Tipi di firma: base, avanzata e qualificata
- Uso della firma nel settore pubblico: previsto
- Siti web: http://www.regtp.de; http://www.isis-mmt.de

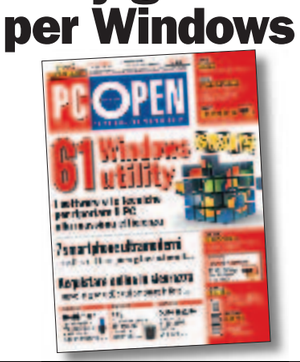
Olanda
- Tipi di firma: base
- Uso della firma nel settore pubblico: non previsto
- Siti web: http://www.ecp.nl ; http://opta.nl

Regno Unito
- Tipi di firma: base e avanzata
- Uso della firma nel settore pubblico: previsto
- Siti web: http://dti.gov.uk; http://www.gateway.gov.uk

Spagna
- Tipi di firma: base, avanzata e qualificata
- Usa della firme nel settore pubblico: previsto
- Siti web: http://www.congresso.es; http://mcyt.es; http://www.sesti.mcyt.es

DOSSIER A CURA DI
Antonello Cherchi

Speciale
utility gratuite
per Windows



In edicola con PC Open di ottobre

Il Sole-24 Ore
Lunedì 8 Ottobre 2007 - N. 276

Atti informatici

GLI STRUMENTI

Il kit. È composto dalla smart card e da un lettore che va collegato al computer

Il sistema. Due chiavi, una pubblica e una privata, che devono combaciare

Come funziona

1. Per disporre del kit della firma digitale l'utente si reca presso la sede di uno dei certificatori accreditati con un documento d'identità valido e firma il contratto

2. Ritira il kit per la firma digitale, composto da una smart card e un lettore da collegare al Pc. Vedi esempio

3. Collega il lettore di smart card al computer e installa l'apposito software fornito dal certificatore

4. Per firmare un documento, lo apre (per esempio, da Word) e seleziona il comando «Firma»

5. Salva il documento firmato. All'estensione normale (doc, pdf, eccetera) il programma aggiunge l'estensione .p7m, che contraddistingue i documenti sottoscritti con la firma digitale

6. Il documento può esser inviato tramite la normale e-mail oppure pubblicato su un sito Web

7. Un altro utente che volesse verificare la firma digitale deve aprire il file firmato con un software simile al primo (quello della firma), il quale, per prima cosa, mostra tutti i dati del firmatario e dell'ente certificatore

8. Il software analizza anche l'integrità del documento e la validità del certificato. Se la verifica è positiva, visualizza un messaggio del tipo «Verifica completata correttamente»

La «sigla» si divide in tre

In realtà la firma utilizzata è soltanto la sottoscrizione digitale

Paolo Subioli

Agli albori di Internet si diceva: «Nella Rete, nessuno sa che sei un cane", per intendere che dove gli interlocutori non possono essere condizionati dall'aspetto fisico o dal pregiudizio, chiunque ha pieno diritto di parola. Presto però è sorta la necessità di identificare con certezza le persone, perché si è visto che la Rete non è fatta solo per scambiare idee, ma anche per vendere, comprare e sottoscrivere contratti a distanza.

L'atto dell'autenticazione, che consiste nel dichiarare il proprio nome utente e associargli la password, è sufficiente nella grande maggioranza dei casi (uno dei quali è l'uso dell'e-mail). L'innovazione tecnologica ha, però, escogitato anche un metodo infallibile per associare un certo documento a una e una sola persona: la firma digitale o, in gergo tecnico, "crittografia a chiavi asimmetriche", la quale consente di risalire con certezza all'autore di un dato documento, che in tal modo assume lo stesso valore legale di una tradizionale firma apposta su carta.

La doppia chiave

Il titolare di firma digitale dispone di una coppia di chiavi, una privata - segreta e custodita sulla smart card e protetta da un codice di accesso (Pin) - l'altra pubblica - custodita e pubblicata dall'ente certificatore - la quale viene usata per la verifica della firma. Le due chiavi sono correlate in maniera univoca, ma dalla chiave pubblica è impossibile risalire a quella privata.

Il meccanismo della doppia chiave consente sia di risalire con certezza all'identità del sottoscrittore, sia di avere la garanzia che il documento informatico non sia stato manomesso dopo la sua sottoscrizione. Inoltre, un documento firmato digitalmente non può essere in alcun modo "ripudiato" dal sottoscrittore.

Il funzionamento del sistema è garantito dalla presenza di una terza parte fidata - l'ente certificatore - che assicura l'associazione univoca tra la chiave pubblica da usare per la verifica e il titolare della corrispondente chiave privata. Tale associazione si basa sull'emissione di un certificato digitale, che avviene solo dopo l'identificazione e registrazione certa del richiedente. Il certificatore gestisce l'intero ciclo di vita del certificato, compresa la sospensione temporanea della sua validità o la revoca definitiva.

Il kit di firma

Per firmare digitalmente un documento occorre un apposito dispositivo elettronico, che consenta di conservare in modo protetto le chiavi private del titolare e di generare al suo interno la firma digitale. Il tipico dispositivo di firma è una smart card, che di solito viene fornita dal certificatore assieme a un apposito lettore da collegare al computer. Un'interessante alternativa è costituita da una chiave Usb - come la Business key rilasciata da Infocamere - con dentro tutti gli strumenti necessari per firmare digitalmente i documenti. Il vantaggio è la completa portabilità, il non richiedere l'installazione e la possibilità di includere nella chiavetta sia gli stessi documenti firmati, sia tutte le applicazioni necessarie.

Con la forma digitale si può sottoscrivere qualsiasi tipo di documento: doc, rtf, txt, pdf, tif, htm, xls. L'unico formato che non viene trasformato con la firma è il pdf, riconosciuto dalla normativa italiana come pienamente valido ai fini della firma digitale.

Il certificato digitale rilasciato dal certificatore può consentire anche altri utilizzi, come firmare la propria posta elettronica o autenticarsi ai siti web in modalità sicura.

Tre tipologie

La normativa prevede in teoria tre diversi tipi di firma: "firma elettronica", "firma elettronica qualificata" e "firma digitale". La prima è un qualunque sistema di autenticazione, quindi comprende tutti i tipi di accesso con semplice nome utente e password. Di fatto, è il sistema più diffuso di riconoscimento, sia in ambito e-commerce, sia nei servizi degli enti pubblici.

La "firma elettronica qualificata" è invece definita come una firma elettronica basata su una procedura che permetta di identificare in modo univoco il titolare, attraverso mezzi di cui il firmatario detenga il controllo esclusivo, e la cui titolarità sia certificata da un soggetto terzo.

La "firma digitale", è considerata dalla legge come una particolare specie di "firma elettronica qualificata", basata sulla tecnologia della crittografia a chiavi asimmetriche. Tale impostazione è però solo teorica, perché, nella realtà concreta, la firma digitale è l'unico tipo di firma elettronica avanzata oggi conosciuto e utilizzato.

Il glossario

Autenticazione informatica
Dizione generica che indica la validazione dell'insieme di dati attribuiti in modo esclusivo e univoco a una persona, per distinguerne l'identità nell'ambito dei sistemi informativi, effettuata attraverso opportune tecnologie, al fine di garantire la sicurezza dell'accesso

Carta d'identità elettronica
Il documento d'identità, munito di fotografia del titolare, rilasciato su supporto informatico dalle amministrazioni comunali, con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare

Carta nazionale dei servizi
Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni

Certificati elettronici
Gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità informatica dei titolari stessi

Certificatore
Il soggetto, iscritto all'elenco pubblico tenuto dal Cnipa, che presta servizi di certificazione delle firme elettroniche e che generalmente fornisce altri servizi a esse collegati

Chiave privata
L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico

Chiave pubblica
L'elemento della coppia di chiavi asimmetriche destinato a essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche

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 (ad esempio, nome utente e password)

Firma elettronica qualificata
Definizione solo teorica, che indica la firma elettronica ottenuta attraverso una procedura informatica che garantisca la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati. Un tipo specifico di firma elettronica qualificata è la "firma digitale"

Firma digitale
Un particolare tipo di firma elettronica qualificata, basata su un sistema di "chiavi crittografiche", una pubblica e una privata, correlate tra loro, che consente rispettivamente al titolare, tramite la chiave privata, e al destinatario, tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico

Posta elettronica certificata (Pec)
È uno degli strumenti informatici che consente la gestione dei documenti in forma digitale. La Pec, in particolare, certifica l'avvenuta spedizione di un messaggio e il relativo orario, al pari della posta raccomandata

Protocollo informatico
L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti

Titolare
La persona fisica cui è attribuita la firma elettronica e che ha accesso al dispositivo per la creazione della firma elettronica

Validazione temporale
Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data e un orario opponibili ai terzi

La certezza dei tempi arriva via mail

Maurizio Pirazzini

La Pec (Posta elettronica certificata) è uno dei pilastri su cui poggia un'infrastruttura per la dematerializzazione dei documenti. Infatti, mantenendo la semplicità d'uso della normale posta elettronica, consente di ottenere, in pochi click, l'equivalente di una raccomandata o addirittura di una notificazione a mezzo posta. Ma tale garanzia è assicurata solo se entrambi gli operatori (mittente e destinatario del messaggio) sono dotati di casella Pec, che costituisce il naturale complemento della firma digitale, strumento non idoneo a garantisce certezza sulla consegna dei documenti informatici. I servizi di Pec possono essere erogati solo da gestori qualificati iscritti nell'elenco tenuto dal Cnipa.

Come funziona

Per ogni messaggio inviato il titolare della casella di Pec – per il quale restano del tutto "trasparenti" gli imbustamenti e le ricevute elettroniche scambiate tra i server dei gestori – dovrà gestire sostanzialmente due tipologie di ricevute: la ricevuta di accettazione, rilasciata dal gestore del mittente all'atto della presa in carico del messaggio, che costituisce prova dell'avvenuta spedizione; la ricevuta di avvenuta consegna rilasciata dal gestore Pec del destinatario, la quale costituisce prova che il messaggio è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario.

La ricevuta di consegna potrà essere: completa, nella quale sono indicati i dati di certificazione e il messaggio originale comprensivo degli allegati (in questo la Pec, a differenza della raccomandata cartacea, crea un legame inscindibile tra la busta e il suo contenuto); breve, nel caso in cui il messaggio sia documentabile solo per estratto; sintetica, se contiene i soli dati di certificazione.

In caso di mancata consegna entro le 24 ore dalla spedizione o in caso di accertamento di virus informatici, al mittente sarà recapitato un avviso di mancata consegna con indicazione della motivazione.

Il singolo messaggio di Pec è garantito dall'utilizzo di una firma elettronica del gestore oltre che dall'apposizione di uno specifico riferimento temporale opponibile ai terzi.

Il valore giuridico

A differenza della semplice e-mail, il cui valore giuridico è oggetto di un acceso dibattito dottrinale e giurisprudenziale, la Pec (specie se in accoppiata con la firma digitale apposta sui documenti allegati), si prospetta come lo strumento destinato a rivoluzionare le modalità di trasmissione dei documenti giuridicamente rilevanti sia nei rapporti tra privati sia nei confronti della pubblica amministrazione. Per poche decine di euro all'anno chiunque, tramite Internet, potrà inviare e-mail "raccomandate" oltre che effettuare vere e proprie notificazioni di documenti informatici che saranno, di regola, validati con l'utilizzo della firma digitale.

La Pec rappresenta così lo strumento di complemento necessario per far decollare l'utilizzo della firma digitale.

Gli uffici pubblici

Il Codice dell'amministrazione digitale conferma l'obbligo da parte delle amministrazione pubbliche di dotarsi di una casella di posta elettronica certificata (connessa al protocollo informatico) che dovrà essere pubblicata sia su un apposito indice centralizzato (www.indicepa.gov.it) che sui siti delle singole amministrazioni. I cittadini possono pertanto pretendere di esercitare il diritto all'uso delle nuove tecnologie verso la pubblica amministrazione, che peraltro dal settembre 2006 sono obbligate a disporre di una casella istituzionale pubblicata.

I costi

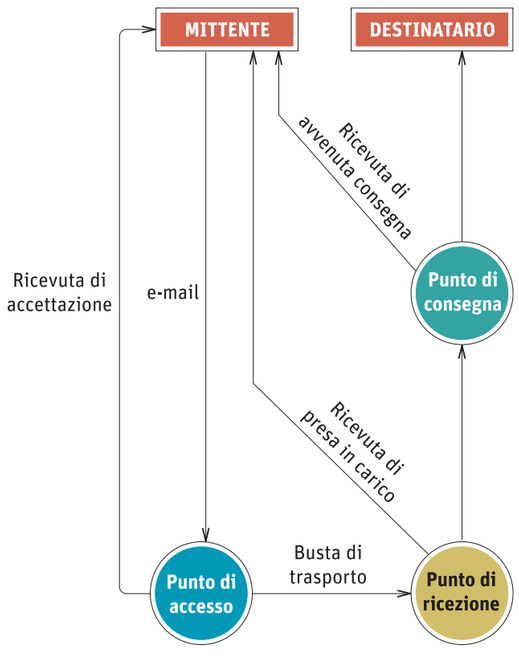
Rispetto al servizio postale cartaceo tradizionale i costi sono inferiori di oltre il 90 per cento. Inoltre non si paga in base alle dimensioni (e al peso) come per le raccomandate tradizionali, senza considerare gli ulteriori costi occulti quali il tempo necessario per compilare la documentazione cartacea, il raggiungimento dell'ufficio postale, l'attesa agli sportelli, la gestione dell'archivio cartaceo ingombrante e difficile da consultare. Tutto spazzato via in pochi click.

A PROVA DI DUBBI
La posta elettronica certificata equivale a una raccomandata e garantisce l'avvenuto recapito del messaggio

I RISPARMI
Rispetto al servizio tradizionale la Pec rende possibile un taglio dei costi superiore al 90 per cento

Dal mittente al destinatario

Il percorso della posta elettronica certificata



I certificatori. Requisiti ferrei

Nell'elenco Cnipa i depositari delle tessere

La legge stabilisce precisi requisiti per l'esercizio dell'attività di certificazione, ai fini della validità legale della firma digitale: vincoli giuridici, di onorabilità dei rappresentanti legali e dei responsabili dell'amministrazione, di competenza ed esperienza dei responsabili tecnici, nonché di conformità di processi e prodotti informatici a standard riconosciuti di qualità. È richiesto inoltre che il soggetto certificatore sia incluso in un elenco pubblico consultabile telematicamente, predisposto, tenuto e aggiornato a cura del Cnipa (si veda la scheda a fianco; l'elenco è aggiornato a luglio 2007).

Per diventare certificatori, bisogna, per esempio, presentare al Cnipa un certificato di iscrizione nel Registro delle imprese con "dicitura antimafia", una copia della polizza assicurativa per la copertura dei danni causati da terzi e copia del piano di sicurezza. Inoltre si deve dare disponibilità a consentire l'accesso a incaricati del Cnipa alle strutture dedicate alla certificazione per verificare la permanenza dei requisiti tecnico-aorganizzativi documentati all'atto di presentazione della domanda.

I certificatori svolgono il ruolo di "terze parti fidate", cioè soggetti terzi che si trovano in posizione di neutralità rispetto agli utilizzatori delle tessere con la firma digitale. Verificano ed attestano, emettendo un apposito certificato digitale, l'identità del titolare ed eventualmente la veridicità di una serie di altre informazioni; stabiliscono il termine di scadenza dei certificati; pubblicano il certificato e la chiave pubblica; ricevono la segnalazione di eventuali smarrimenti, furti, cancellazioni, divulgazioni improprie di chiavi private e pubblicano quindi la lista dei certificati revocati o sospesi in conseguenza di tali fatti.

An. Mari.

L'elenco

Infocamere Sc.p.a.
www.card.infocamere.it

Postecom Spa
www.poste.it

Cnipa - Centro nazionale per l'informatica nella pubblica amministrazione (già centro tecnico per la Rupa)
www.cnipa.gov.it

In.Te.S.A. Spa
http://e-trustcom.intesa.it

Trust Italia Spa
https://firmadigitale.trustitalia.it

Cedacri Spa (già Cedacrinord Spa)
http://www.cedacricert.it

Actalis Spa
http://www.actalis.it

Consiglio nazionale del notariato
http://ca.notariato.it

Comando trasmissioni e informazioni esercito (già Comando C4 - IEW)
www.eicert.esercito.difesa.it

Consiglio nazionale forense
http://ca.consiglionazionaleforense.it

Sogei Spa
http://ca.sogei.it

Sanpaolo Imi Spa
http://ca.sanpaoloimi.com

B. Monte dei Paschi di Siena Spa
http://www.mps.it

Lombardia integrata Spa - Servizi infotelematici per il territorio
http://www.lisit.it

Banca Intesa Spa
http://ca.bancaintesa.it

Banca di Roma Spa
http://www.bancaroma.it

I.T. Telecom Srl
http://www.firmasicura.it

Consorzio Certicomm (autorità di certificazione dei Consigli nazionali dei ragionieri e dei dottori commercialisti)
http://www.certicomm.it

Comando C4 Difesa - Stato maggiore della Difesa
www.pkiff.difesa.it/

Infocert Spa
www.infocert.it

La diffusione. Gli usi comuni

Riconosciuti con la password

C'è chi gira ancora con la stilografica nel taschino: un vezzo che ne rende la firma più elegante e inimitabile. Invece di quelli che si portano appresso una smart card con la propria firma digitale non se ne vedono molti, dal momento che questa forma così moderna di sottoscrizione, nonostante gli indubbi vantaggi, è ancora poco diffusa tra i cittadini comuni. Eppure l'offerta commerciale non manca – essendo una dozzina i certificatori che offrono questo servizio ai privati – e il servizio costa anche poco, non superando di solito i 40 euro.

In generale, la firma digitale serve ogni qual volta sia necessario sottoscrivere documenti o farsi riconoscere in modo inequivocabile a distanza. Ma per le normali transazioni via Internet, come effettuare acquisti e prenotazioni, versare tributi o completare procedure amministrative, si è ormai consolidata la prassi del semplice ricorso all'autenticazione tramite nome utente e password (o Pin), ed è questo il motivo di una diffusione circoscritta della firma digitale.

Chi comunque desidera dotarsi di questa opportunità, deve recarsi presso la sede di uno dei certificatori accreditati con un documento d'identità valido, per farsi riconoscere e firmare il contratto. Successivamente potrà ritirare il "kit", che consiste tipicamente in una smart card, contenente il certificato digitale in grado di generare la firma, e un relativo lettore da collegare al computer. Il certificato ha una validità di tre anni, ma se ne può ottenere il rinnovo prima della scadenza.

È anche possibile acquistare ulteriori prodotti collegati: la marca temporale, che consente di certificare la data e l'ora associate a un documento informatico, provandone l'esistenza a quella precisa data; il certificato elettronico, destinato alla gestione di siti web, che permette di instaurare una connessione sicura, basata sul protocollo Ssl, tra il server e il browser dell'utente che accede al servizio; i certificati per web server, che permettono di autenticare l'identità del sito al quale ci si collega e della società che ne è titolare, come fanno le banche.

I kit per la firma digitale forniti dai certificatori non servono solo per l'invio di documenti, ma anche per la loro ricezione. Tramite i relativi software, ad esempio, si può verificare la reale identità di chi ha firmato un documento e constatare l'effettiva integrità di quest'ultimo. Oltre ai documenti, è possibile firmare digitalmente anche l'e-mail, uno strumento che altrimenti è molto facilmente falsificabile, nonostante la grande maggioranza degli utenti non ne sia pienamente consapevole.

P. Su.

Atti informatici

I SETTORI

La Lombardia. Ha una propria autorità di certificazione che ha fornito 45mila card

Semplificazioni. Infocamere ha presentato un sistema che si basa su una chiave Usb

Uffici pubblici sempre più digitali

Quest'anno l'uso della firma elettronica è raddoppiato rispetto al 2006

Andrea Marini

Uno strumento ormai indispensabile per la pubblica amministrazione. La firma digitale cresce con incrementi a due cifre e il prossimo anno potrebbe addirittura più che raddoppiare, a seconda dell'entrata a regime della fatturazione elettronica.

Le stime effettuate da Cnipa (il Centro nazionale per l'informatica nella pubblica amministrazione) parlano di oltre 70 milioni di documenti firmati digitalmente da inizio 2007 a oggi (60 milioni il dato certificato dalla sola Regione Lombardia).

Nel 2006 l'utilizzo era di circa la metà (35 milioni, quindi). Ma l'anno d'oro della firma digitale potrebbe essere il 2008: le previsioni si aggirano attorno ai 100 milioni, che potrebbero salire a 150 con l'avvio, appunto, della fatturazione elettronica.

Milano al top

Tra gli enti che nel 2007 ne hanno fatto un uso maggiore c'è stata la Regione Lombardia, che ha anche un'autorità di certificazione propria (Lisit), la quale ha emesso oltre 45mila dispositivi di firma. I numeri riguardano in toto il settore della sanità: dei 60 milioni di documenti, il 90% sono prescrizioni, il 10% referti.

Tra le altre istituzioni emergono l'Arma dei carabinieri, il ministero dell'Economia, la Guardia di finanza e il ministero della Giustizia. Per Via Arenula, si tratta soprattutto degli atti inerenti al processo telematico, mentre i Carabinieri si distinguono per i libri matricola e le buste paga.

In generale, a essere inviati sono bilanci, dichiarazioni fiscali e atti di spesa. A livello di amministrazioni locali, secondo le rilevazioni effettuate nel 2006, sono in possesso di firma digitale il 19,5% dei Comuni (che diventano il 29% nelle realtà con più di 60mila abitanti) e il 47% delle Province.

I risparmi di costi sono evidenti, ragion per cui, al di là dei vincoli di legge, lo sviluppo pare assicurato. Soprattutto nel caso in cui la firma digitale sia abbinata alla posta elettronica certificata (Pec). Il Codice dell'amministrazione digitale obbliga, tra l'altro, le amministrazioni pubbliche a dotarsi di una casella di posta elettronica da pubblicare sul sito www.indicepa.gov.it e sui siti della singole amministrazioni. Entro fine 2008 la posta certificata dovrà essere l'unico mezzo di comunicazione tra gli uffici pubblici.

La Pec conta ormai milioni di messaggi al mese ed equivale legalmente alla raccomandata tradizionale. In genere serve a certificare l'invio di documentazione con una scadenza. Può essere, per esempio, il caso di un avvocato che spedisce degli atti al tribunale, documenti che devono giungere a destinazione entro una data esatta. Ma può essere usata anche per convocare un consiglio di amministrazione.

Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte, conservata per legge per un periodo di 30 mesi, consente la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.

E-mail certificata in crescita

In base ai dati bimestrali forniti dai gestori, dall'inizio dell'attività di vigilanza svolta dal Cnipa, ovvero dal secondo bimestre di quest'anno, a luglio-agosto i domini attivi di posta elettronica certificata sono passati da 4.828 a 8.421. Circa un terzo riguardano la pubblica amministrazione. Un andamento che indica da solo il boom della diffusione presso le organizzazioni pubbliche del servizio. La riduzione del numero di caselle (da 116.585 a 115.483) – spiegano dal Cnipa – può invece essere imputabile al termine di fasi promozionali di lancio che alcuni gestori hanno attivato.

Il trend dell'utilizzo della Pec, a ogni modo, è in sensibile crescita. Nel secondo bimestre 2007 sono stati scambiati circa 14,6 milioni di messaggi. Numero schizzato a 24 milioni a maggio-giugno, sceso a 22,9 a luglio-agosto. Ma nel periodo estivo il calo è fisiologico: nei prossimi mesi, c'è da scommetterci, la corsa riprenderà a ritmo sostenuto.

CORBIS

L'obiettivo. Con le nuove tecnologie sempre meno carta sui tavoli

Via mail

L'evoluzione della posta elettronica certificata

Periodo	Domini	Caselle	Messaggi
Marzo-aprile	4.828	116.585	14.573.203
Maggio-giugno	2.053	6.030	24.047.429
Luglio-agosto	1.540	- 7.132	22.916.619
Totale	**8.421**	**115.483**	**61.537.251**

Fonte: Cnipa (dati 2007)

L'avanzata del bit

Il numero di documenti sottoscritti nel 2007 dalla pubblica amministrazione con la firma digitale

Amministrazioni	Documenti firmati (milioni)
Regione Lombardia	60
di cui:	
referti	6
prescrizioni	54
Carabinieri, ministero Economia, Guardia di Finanza, ministero Giustizia	10
Totale	**70**

Fonte: Cnipa

In azienda

Il numero di pratiche telematiche inviate nel 2007 dalle imprese alle Camere di commercio

Tipologia	Documenti firmati
Bilanci	800.000
Iscrizioni, modifiche, cessazioni	1.600.000
Totale	**2.400.000**

Fonte: Infocamere

Breccia aperta nelle imprese

Ogni anno sono inviate alle Camere di commercio circa 2,4 milioni di pratiche firmate digitalmente, cifra destinata a crescere quando verrà data piena attuazione al cosiddetto provvedimento "impresa in un giorno". Per quel che riguarda i certificati di firma digitale distribuiti, a oggi siamo a 2,6 milioni, mentre per le caselle di posta elettronica certificata "Legalmail" siamo a 70mila. Tra le imprese, quindi, i nuovi strumenti di autenticazione sicura a servizi web di e-government sono ormai diventati pane quotidiano.

In dettaglio, dei 2,4 milioni di pratiche telematiche, 1,6 milioni sono relative a iscrizioni, modifiche o cessazioni di attività; le restanti 800mila sono invii di bilanci. Sul fronte dei certificati di firma digitale finora emessi (2,6 milioni), essi appartengono per circa il 70% alle imprese e per il restante 30% a professionisti e altri utenti (ad esempio le pubbliche amministrazioni centrali e locali). I titolari delle 70mila Legalmail sono l'84,5% imprese, il 6,6 professionisti, il 3,6 associazioni, seguiti da pubbliche amministrazioni locali (1,8) e centrali (0,7), privati cittadini (0,3) e altri soggetti non indicati nel dettaglio (2,4).

LE PRATICHE SUL WEB
Sono circa 2,4 milioni quelle inviate ogni anno alle Camere di commercio per iscrizioni, modifiche o cessazioni di attività

La novità di InfoCert (controllata di Infocamere, la società consortile di informatica delle Camere di commercio italiane) in materia di firma digitale si chiama Business key. Lo strumento consente agli amministratori di impresa e al loro personale operativo di rendere disponibili le applicazioni e i documenti necessari a completare le attività ovunque si trovino. I dispositivi di firma digitale e gli strumenti di autenticazione sicura a servizi web di e-government attualmente distribuiti sono, infatti, considerate dagli imprenditori di non sempre facile utilizzo: le smart card necessitano di un lettore apposito e di una procedura articolata di installazione e hanno il limite di non essere "portabili", in quanto presuppongono che ci sia una stazione di lavoro già predisposta per il loro utilizzo. Business key, invece, è una "chiavetta" Usb che contiene l'applicazione per la sottoscrizione informatica.

Uno degli usi più diffusi della firma digitale da parte di imprenditori e professionisti è l'invio delle pratiche telematiche al Registro delle imprese delle Camere di commercio attraverso il servizio Telemaco, che permette anche l'accesso alle informazioni sullo stato di avanzamento della pratica stessa. Con Telemaco è possibile effettuare, via Internet, la spedizione di domande quali, ad esempio, l'iscrizione, la modifica e la cessazione di un'attività. L'invio equivale alla presentazione a mezzo plico raccomandato.

Una volta compilato il modello e gli allegati che compongono la pratica, il documento, sottoscritto con la firma digitale, viene trasmesso via Internet al Registro imprese attraverso protocolli di invio e ricezione sicuri. Le funzioni presenti nel servizio di spedizione sono l'invio delle pratiche, il deposito dei bilanci e l'assegnazione della partita Iva.

La posta elettronica certificata Legalmail permette invece di sostituire la raccomandata, il fax o altri strumenti tradizionali nei rapporti ufficiali con soggetti che dispongono di posta certificata e per l'inoltro di comunicazioni che attestino l'invio ma non richiedano la certificazione della consegna. È il caso, per esempio, di ordini, contratti, fatture, trasmissione di documenti alle pubbliche amministrazioni, convocazioni di consigli, assemblee e giunte. E ancora: inoltro di circolari e direttive, gestione di gare di appalto, gestione delle comunicazioni ufficiali all'interno di organizzazioni articolate o a "rete" (franchising, agenti), integrazione delle trasmissioni certificate in altri prodotti, come paghe e stipendi, protocollo, gestione di documenti.

An.Mari.

Giustizia. Il traguardo del 2010

Le carte del processo civile viaggiano online

Giovanni Parente

Nel processo telematico, i problemi legati all'incompatibilità della firma digitale sono in via di superamento. Anche se ci sono state «grosse difficoltà» come ammette Sergio Brescia, a capo della Direzione generale per i sistemi informativi automatizzati (Dgsia) del ministero della Giustizia. Ormai però «i certificatori hanno raggiunto uno standard che assicura l'interoperabilità», garantisce Floretta Rolleri, componente del Cnipa.

SOTTO ESAME
Avvio legato al disegno di legge del Governo, ora all'esame del Parlamento, che detta i tempi per la trasformazione

Adesso il futuro del processo telematico si gioca in Parlamento. Se passerà il disegno di legge varato dal Governo lo scorso 23 maggio (e presentato alla Camera il 5 luglio), il 30 giugno 2010 sarà la data in cui diventerà operativa la completa digitalizzazione dei procedimenti civili come le ingiunzioni, le esecuzioni immobiliari e le controversie in materia di previdenza e assistenza obbligatoria. Per lo stesso giorno, ma del 2009, è fissato nell'iniziativa legislativa dell'Esecutivo il termine da cui le notifiche dovrebbero viaggiare solo on line.

Un passaggio ritenuto fondamentale da Brescia: «La notifica normale deve essere quella della casella certificata». Altrimenti, in assenza di uno specifico obbligo, «continuerà a esistere il regime del doppio binario». Ma non è il solo nodo da sciogliere. Perché in attesa che il Ddl segua il suo iter parlamentare, sono necessari investimenti in infrastrutture e organizzazione.

L'obiettivo è di realizzare e rendere «affidabile a tutti gli effetti» una sala server per ogni distretto di Corte d'appello. «Se dalla Finanziaria 2008 – puntualizza Brescia – avremo i fondi necessari, in un anno ci saranno sale attrezzate in tutta Italia». Una volta disponibile l'hardware, si dovrà poi intervenire sulle capacità di impiego. «Bisognerà accompagnare – aggiunge – l'ufficio nell'utilizzo della tecnologia con un trasferimento di know how dal centro ai distretti locali».

È stato il Dpr 123/2001 a regolamentare l'introduzione del processo telematico. Dalla fine del 2004 sono partite le sperimentazioni in sette tribunali. Tra questi non c'era Milano, dove invece dallo scorso 11 dicembre si è cominciato a fare sul serio con l'invio del primo decreto ingiuntivo dotato di valore legale. L'Ordine degli avvocati meneghino ha spinto notevolmente sul progetto, credendo sulle potenzialità soprattutto in termini di taglio dei tempi.

Il legale, con l'iscrizione al Punto di accesso e con a disposizione una smart card e una firma digitale (che può essere rilasciata dall'Ordine o da un altro certificatore), è in grado di siglare gli atti e inviarli attraverso una casella elettronica, utilizzabile solo per questa finalità, direttamente agli uffici giudiziari. Dalla cancelleria poi avviene la trasmissione al giudice, che avrà a disposizione il fascicolo informatico. Una volta emesso, il provvedimento segue il percorso inverso, sempre però attraverso l'e-mail certificata. Le stime per i primi sei mesi, relative ovviamente solo ai decreti ingiuntivi, valutano un abbattimento dai 60 giorni per la procedura cartacea a un massimo di 15 per quella telematica. Con un risparmio stimabile in 14 milioni di euro all'anno.

La sperimentazione

I passaggi che porteranno al processo telematico

- Il Dpr 123/2001 ha disciplinato l'utilizzo degli strumenti informatici e telematici nel processo civile, amministrativo e davanti alle sezioni giurisdizionali della Corte dei conti
- L'avvio della sperimentazione sull'invio di atti relativi a procedimenti civili attraverso caselle di posta certificata è iniziata negli ultimi mesi del 2004 e ha riguardato sette tribunali
- Solo presso il tribunale di Milano (che non faceva parte del novero dei distretti sperimentali) i decreti di ingiunzione trasmessi con modalità elettroniche hanno iniziato ad avere valore legale a partire dal dicembre 2006
- Per poter accedere ai servizi disponibili telematicamente gli avvocati devono dotarsi di smart card contenenti il certificato per la firma elettronica (rilasciato da un certificatore accreditato) e il certificato di autenticazione, per la connessione al punto di accesso
- Il sistema delle notifiche elettroniche è strutturato secondo un flusso bidirezionale con l'invio di un biglietto di cancelleria tramite la trasmissione di una comunicazione del cancelliere alle caselle di posta elettronica del processo telematico di uno o più avvocati e con una risposta di ritorno innescata dall'emissione delle singole ricevute di presa in carico dei messaggi

Professionisti. La tecnologia avanza negli studi

Utilizzo a tutto campo: dal Catasto alle assunzioni

Nel 2006 i notai hanno effettuato per via telematica 21,5 milioni di visure (cioè controlli e accertamenti) e 2 milioni di invii di documenti. Il settore, ormai è avviato sempre più nella gestione dei documenti in forma elettronica, con l'obiettivo di rendere efficiente il rapporto con la pubblica amministrazione. Gli investimenti realizzati sono stati considerevoli, sia per i contributi di studio diretti ad assicurare piena validità giuridica ai processi innovativi, sia per gli investimenti tecnologici (al 2006 oltre 5 milioni di euro: 3,3 milioni di hardware e 1,7 di software), senza alcun costo a carico dello Stato.

BATTISTRADA
I notai sono la categoria più avanzata per diffusione dei nuovi strumenti: nel solo 2006 hanno investito 5 milioni di euro

Oggi, la totalità degli atti notarili è trasmessa digitalmente all'Agenzia delle entrate, agli Uffici del territorio e ai Registri delle imprese. La firma digitale del notariato differisce da quelle rilasciate dagli altri certificatori perché, oltre a garantire l'identità del firmatario, ne certifica la funzione notarile, garantisce cioè che il firmatario è un notaio nell'esercizio delle sue funzioni.

In particolare, l'anno scorso sono state effettuate 10 milioni di visure ipotecarie, 7 milioni di visure catastali, 4,5 milioni di visure camerali, 2 milioni di invii telematici, grazie alla la Run, la Rete unitaria del notariato che collega fra loro e con la pubblica amministrazione la totalità degli studi notarili. Con le visure catastali vengono verificati dati identificativi relativi agli immobili, mentre con quelle ipotecarie vengono svolti i controlli sulla titolarità degli immobili e la verifica sull'inesistenza di ipoteche, pignoramenti o di altri vincoli che possano mettere a rischio la proprietà dell'immobile. Le visure camerali riguardano invece gli accertamenti relativi alle imprese e vengono effettuati con collegamenti telematici con le Camere di commercio.

Sul fronte dei circa 2 milioni di invii telematici, quelli riguardanti gli atti immobiliari (1,2 milioni) sono stati trasmessi all'Ufficio del territorio, che ha la competenza di Conservatoria e Catasto, mentre quelli alle imprese (oltre 650mila) sono stati trasmessi alle Camere di commercio. L'estensione dal 1° aprile 2007 della registrazione telematica a tutti gli atti notarili ha portato un trend di crescita tra il 70 e l'80 per cento degli invii telematici. Le previsione per la fine dell'anno è di circa 3 milioni, e per il 2008 di circa 3,5 milioni.

Anche tra gli avvocati la firma digitale si è ritagliata i propri spazi, che non sono solo quelli del futuro processo telematico (si veda l'articolo sopra). «Non è possibile determinare quanti documenti siano stati firmati digitalmente – afferma Massimo Melica, segretario generale della Fondazione per l'informatica e l'innovazione forense, presso il Consiglio nazionale forense (Cnf) – tuttavia la diffusione nell'Avvocatura del kit per la firma digitale, rilasciato dal Cnf, è in continua crescita e ha raggiunto in pochi anni circa 7mila utenti».

«Oggi – continua Melica – il professionista forense utilizza per lo più la firma per accedere a servizi telematici istituzionali, ma anche per la tenuta di registri digitali o per lo scambio di atti con i colleghi, unendo alla firma digitale lo strumento della posta elettronica certificata».

Il dispositivo di firma digitale è oggi utilizzato invece negli studi dei dottori commercialisti e dei ragionieri prevalentemente per la sottoscrizione delle istanze e delle domande di deposito degli atti societari al Registro delle imprese. A partire dal 2005 in diverse realtà provinciali lo strumento della firma digitale è utilizzato anche per le comunicazioni di assunzione del personale da parte delle aziende. È il commercialista che se ne occupa e che sottoscrive con il proprio dispositivo di firma la comunicazione di assunzione.

An. Mari.

Il fenomeno

1.000
Firme digitali
Sono i documenti che un notaio firma mediamente in un anno con la sottoscrizione elettronica

7.000
Dispositivi di firma
È il numero di utenti che ha chiesto un kit di firma digitale al Consiglio nazionale forense, che è iscritto all'elenco del Cnipa come autorità di certificazione

70.000
Carte
Sono le smart card di firma digitale in possesso dei dottori commercialisti e dei ragionieri

Fisco. Nel nome della semplificazione

Per pagare le imposte basta inviare un file

Alessandro Mastromatteo
Benedetto Santacroce

L'utilizzo della firma digitale è espressione non solo di obblighi ma anche di sempre maggiori opportunità in termini di semplificazione e razionalizzazione dei rapporti e degli adempimenti tra contribuenti e Fisco. Si consideri che l'Agenzia delle dogane, pur nelle difficoltà di ordine pratico di abbandonare il supporto cartaceo a favore di quello informatico, sta progressivamente riconoscendo la piena validità di dichiarazioni telematiche inviate e sottoscritte con la firma digitale.

ARCHIVI SNELLI
La conservazione sostitutiva consente di trasferire in supporti informatici i documenti rilevanti per l'amministrazione

La firma digitale costituisce una delle modalità, certamente quella di più semplice utilizzo, per l'autenticazione obbligatoria di tutta una serie di documenti predisposti dagli intermediari abilitati utilizzando modalità informatiche, ai fini dell'invio telematico all'Agenzia delle entrate tramite il servizio Entratel.

Devono essere obbligatoriamente autenticati con dispositivo di firma digitale non solo le dichiarazioni dei redditi e i modelli di pagamento F24, ma anche i contratti di locazione, i questionari degli studi di settore, le dichiarazioni d'inizio, cessazione o variazione attività, le denunce nominative degli assicurati Inail e le comunicazione dei dati relativi alle forniture di documenti fiscali. Una volta redatto il documento, i relativi dati devono essere convertiti nel formato previsto per la trasmissione telematica, autenticando con firma digitale il file da inviare.

Le opportunità di semplificazione e razionalizzazione offerte dalla conservazione sostitutiva dei documenti fiscalmente rilevanti, come previsto dal decreto ministeriale 23 gennaio 2004, costituiscono un ulteriore campo di operatività della firma digitale che, unitamente alla marca temporale, rappresenta un elemento indispensabile per procedere alla dematerializzazione degli archivi cartacei.

Anche in ambito doganale risulta sempre più massiccio il ricorso alla firma digitale, con conseguente abbandono del supporto cartaceo. Con l'applicazione Intr@Web OnLine, tramite il sito Internet del sistema telematico doganale (Edi), i soggetti obbligati possono compilare e inviare on line gli elenchi riepilogativi delle cessioni e degli acquisti intracomunitari di beni (modelli Intrastat), firmandoli digitalmente e ricevendo in risposta dall'Agenzia delle dogane il numero di protocollo.

Al fine di monitorare la movimentazione delle merci, tramite il nuovo sistema Ecs (Export control system), le dichiarazioni di esportazione (modello Dau) possono essere presentate non solo su modello cartaceo, da acquisire sul sistema Aida, ma anche mediante l'invio di una dichiarazione telematica con firma digitale.

Il Sole-24 Ore
Lunedì 8 Ottobre 2007 - N. 276

Atti informatici

LA SICUREZZA

Regole auree. Utilizzare personalmente il dispositivo di firma e aggiornare il Pc

La prova. I documenti digitali sottoscritti elettronicamente hanno valore in giudizio

Sistema a prova di hacker

Per violare la metodologia italiana necessario un super-hardware

Maurizio Pirazzini

Un documento con firma digitale a norma di legge è, in linea di massima, un documento più sicuro rispetto al documento cartaceo, a condizione che vengano rispettate alcune regole fondamentali. Per esempio, utilizzare personalmente il dispositivo, non fornire a terzi il Pin, aggiornare il computer su cui si utilizza la firma digitale.

I nuovi strumenti (quali chiavi Usb) contribuiscono a rendere più semplice, portabile e usabile la firma digitale, senza necessità di disporre di un Pc con lettore e software ad hoc preinstallato.

I LATI VULNERABILI

Più facile carpire il Pin di accesso alla chiave privata memorizzata sulla smart card approfittando della disattenzione del titolare

Ma gli "attacchi" al documento elettronico possono riguardare diversi fronti. Il sistema italiano della firma digitale è basato su infrastrutture Pki (Public key infrastructure) che si fondano sulla cosiddetta crittografia a chiave pubblica.

I documenti con firma digitale sono "costruiti" con l'utilizzo di algoritmi sicuri, su cui si basa il tradizionale formato ".p7m" a cui recentemente si sono affiancati formati più diffusi e "standard" quali il ".pdf" e più recentemente il formato ".xml".

Un attacco per scardinare le chiavi è un affare da scienziati che richiede l'utilizzo di risorse hardware impressionanti e per tempi lunghissimi, incompatibili con l'obiettivo di disporre di una firma digitale "falsa".

Molto più subdoli (e facili da implementare) sono gli attacchi basati sulla possibilità di carpire le credenziali di accesso alla chiave privata memorizzata nella smart card o nel dispositivo Usb (il classico Pin scritto sulla smart card). È del tutto illogico - ma purtroppo si verifica spesso nella realtà - lasciare il proprio Pin e la propria smart card presso un soggetto terzo che potrà agire come se fosse il titolare della firma senza alcuna possibilità di dimostrare – dal punto di vista tecnico – la falsità del documento.

Il problema dell'utilizzo "impersonale" – a cui si potrà porre un freno solo con tecniche biometriche – del dispositivo di firma è molto rilevante, anche se spesso la firma digitale viene percepita in modo distorto e non come strumento di firma valido e rilevante a ogni effetto di legge sia per i rapporti privati che nei confronti della pubblica amministrazione. Non infrequente, ad esempio, una percezione da parte delle imprese come strumento utilizzabile "solo" per depositare i bilanci alla Camera di commercio.

La sicurezza è un processo che ha il proprio anello debole non certo nella tecnologia, ma nell'utilizzatore finale, che spesso non si cura di custodire personalmente sia lo strumento (chiavetta Usb o smart card) sia i codici di accesso (Pin). Per non parlare dell'utilizzo della firma digitale in ambienti non sicuri (sistema operativo non aggiornato o protetto da accessi indesiderati che consentano di utilizzare la smart card da remoto) o dell'utilizzo di formati di file non sicuri e immodificabili, in cui sia possibile, ad esempio, inserire un codice eseguibile all'interno del file che può far cambiare date, numeri e importi senza che la firma sia tecnicamente compromessa.

MARKA

Davanti al giudice

Firma elettronica
- Un documento informatico sottoscritto con la firma elettronica – cioè con il tipo "leggero" di sottoscrizione – è liberamente valutabile in giudizio. L'autorità giudiziaria deve tener conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del documento

Firma elettronica qualificata
- Un documento informatico sottoscritto con la firma elettronica qualificata – che rappresenta un tipo di sottoscrizione "pesante" – ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria

Firma digitale
- Un documento sottoscritto con la firma digitale ha lo stesso valore probatorio della firma elettronica qualificata. Dunque, vale l'articolo 2702 del codice civile, il quale dispone che la scrittura privata fa piena prova, a querela di falso, della provenienza delle dichiarazioni di chi l'ha sottoscritta

Per gli usi fraudolenti la sanzione è «generica»

Gianluigi Ciacci

Quali sono le conseguenze per un uso non corretto degli strumenti di firma digitale e, prima ancora, quali ipotesi in concreto di abuso si possono immaginare, soprattutto alla luce della presunta sicurezza tecnica di tali strumenti? L'argomento è di particolare interesse, se si tiene presente che, secondo alcuni commentatori e interpreti, dovrebbe addirittura considerarsi reato un comportamento non così improbabile come quello di fare usare la propria smart card alla segretaria per firmare un documento informatico!

Tenendo presente che nell'ambito della disciplina legislativa in materia, le norme particolari dedicate a tale argomento riguardano solo le responsabilità di natura civile del titolare – che «è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ed a custodire e utilizzare il dispositivo di firma con la diligenza del buon padre di famiglia», articolo 32, comma 1, del Codice dell'amministrazione digitale: nel caso tale regola non sia rispettata, il titolare deve risarcire i danni – e che quindi non esistono specifici reati legati all'uso, o all'abuso, delle firme elettroniche, occorrerà ricercare la risposta nelle regole generali, in particolare in quelle penalistiche.

Le fattispecie

Per far questo è opportuno procedere a un'iniziale indagine circa le diverse possibilità legate all'utilizzo fraudolento delle firme digitali: è possibile quindi distinguere le ipotesi in cui il kit di firma costituisca lo strumento per compiere attività illecite dalle ipotesi in cui oggetto dell'attività sia invece o lo stesso sistema di firma, o il documento firmato.

Nel primo caso, che potremmo ulteriormente distinguere a seconda che il soggetto che agisce sia o meno il titolare del kit (perché lo ha rubato e violato, o perché gli è stato dato in uso), il riferimento alle conseguenze del comportamento dovrà farsi alla specifica disciplina dell'attività illecita posta in essere. Così, ad esempio, se chi procede alla notificazione del trattamento di dati personali, ai sensi dell'articolo 37 del Codice della privacy (adempimento che deve obbligatoriamente avvenire in via telematica con firma digitale), dichiara false notizie, subirà le conseguenze sanzionatorie stabilite nell'articolo 168 della stessa legge: la reclusione da 6 mesi a 3 anni.

L'uso (strumentale) del kit è dunque assorbito dal reato di falsa notificazione.

Ma l'ipotesi che maggiormente interessa riguarda le attività illecite che possono essere compiute specificamente sul "sistema di firma", cioè sul dispositivo, sul certificato, sul documento firmato. Anche in questo caso, ammettendo a livello tecnico che la violazione dell'apparato crittografico alla base dello strumento di sottoscrizione elettronica sia possibile e agevole, si devono ricercare le disposizioni che sono state dettate per fattispecie simili: situazione che è connaturata alla modalità stessa con cui è stato introdotto nel nostro Paese l'attuale sistema di validazione giuridica dei documenti informatici.

Infatti, la "rivoluzione" è stata realizzata estendendo il concetto stesso di documento e di sottoscrizione, senza dover modificare l'impianto normativo esistente: non più realtà solo materiale, caratterizzata dalla carta, dall'autografia, ma anche immateriale, costituita da byte, imputabile in quanto tecnicamente di uso esclusivo; non più documento-"pezzo di carta", ma anche documento-"file".

Atti falsi

Conseguenza di ciò è quindi quella di applicare all'ipotesi in esame non solo la peculiare norma sulla falsificazione del documento informatico (articolo 491-bis del codice penale), ma anche quelle più generali della falsità in atti: l'articolo 485 sulla falsità in scrittura privata, gli articoli 476-480 per le falsità, materiali o ideologiche, del pubblico ufficiale, gli articoli 481-483 per quelle degli esercenti pubblici esercizi o dei privati, sempre che si considerino sostituibili le forme tradizionali cartacee di certificati e autorizzazioni amministrative.

Ipotesi particolari possono poi riguardare altre norme del codice penale, come quelle delle falsità in sigilli, strumenti o segni di autenticazione, certificazione o riconoscimento (articolo 467 e seguenti del codice penale: si pensi alle fattispecie in cui l'uso fraudolento riguar-

PUNIRE GLI ILLECITI

La normativa prevede ipotesi specifiche solo sul versante civile mentre in caso di reati si è fermi al Codice penale

di un dispositivo di firma di un notaio o di altro pubblico ufficiale), quella sulla sostituzione di persona (articolo 494, norma che si potrebbe applicare proprio nel caso di utilizzo abusivo del kit di firma da parte di persona diversa dal titolare) o quelle sul furto o sull'appropriazione indebita (articolo 624 o articolo 646 nel caso di sottrazione dello stesso kit).

Gli altri reati

Ulteriori ipotesi delittuose possono poi ricostruirsi grazie alla specifica attività tecnica che può essere svolta sugli strumenti di firma, sempre comunque riconducibili alle ipotesi delittuose più o meno "tradizionali": dalla truffa, alla ricettazione, all'accesso abusivo a un sistema informatico.

CHI TI OFFRE DI PIÙ?

La Banca Dati del Commercialista GOLD

LA PIÙ COMPLETA E VANTAGGIOSA

• PIÙ ARGOMENTI: Fisco, Società, Contabilità e Bilancio, Fallimento e Procedure concorsuali, Adempimenti.
• PIÙ CONTENUTI: Documentazione ufficiale, Sintesi operative, Dottrina, Commenti d'Autore.
• PIÙ SERVIZI E UTILITÀ: Newsletter, Circolari Aristeia, Guide Pratiche, Prontuario IVA, Formulari, Scadenzari, Programmi di Calcolo, Modulistica, Tabelle, Cartelle personali e molto altro ancora.
• PIÙ AGGIORNATA: ricerche in DVD con "aggiornamenti quotidiani" on-line grazie ad un sistema di consultazione esclusivo.

E-LEARNING CON CREDITI FORMATIVI

LA BANCA DATI DEL COMMERCIALISTA GOLD si arricchisce di contenuti e servizi che nascono dalle collaborazioni con:

ARISTEIA

• E-LEARNING CON CREDITI FORMATIVI: comodamente attraverso il PC gli abbonati possono accedere ai momenti formativi e acquisire i crediti richiesti dal nuovo regolamento di formazione professionale.

PER MAGGIORI INFORMAZIONI
CHIAMA SUBITO: TEL. 02.3022.5670
O COMPILA LA RICHIESTA INFORMAZIONI
ALL'INDIRIZZO www.agenti24.it/bdcgold

Il Sole 24 ORE
www.ilsole24ore.com