UNIVERSITÀ DEGLI STUDI DI PAVIA – SEDE DI MANTOVA

Anno Accademico 2006-2007

CORSO DI SISTEMI INFORMATIVI (DOCENTE DR. RUGGERO FERRARI)

La firma digitale

(Aspetti normativi italiani ed europei)

PRESENTAZIONE DI FRANCO VAROLI

Mantova, 17 maggio 2007

Sommario

Premessa

Era il 1996, "lontano" informaticamente parlando dall'attuale 2007, ed insegnavo Topografia presso l'Istituto Tecnico per Geometri "Carlo d'Arco" di Mantova. Il Dirigente mi affidò l'incarico di tenere dei corsi di approfondimento in merito ad argomenti che riguardassero il mio insegnamento e da svolgere su Personal Computer (d'ora in poi PC). Ricordo che i PC vennero introdotti "ufficialmente" nelle scuole a metà circa degli anni '80, se escludiamo qualche prototipo isolato apparso qualche anno prima. "Ufficialmente" significa che c'era un piano ministeriale che avrebbe dovuto aiutare l'informatizzazione di massa degli operatori ed utenti scolastici.

Nei due lustri circa trascorsi fin al 1996 i PC si evolsero in maniera graduale ma piuttosto lenta, rispetto alla situazione attuale e sempre usando, come unità di misura, il metro informatico. In qui tempi era normale vedere arrivare in laboratorio studenti e docenti con dischetti e CD-ROM contenenti di tutto e di più ed installare arbitrariamente programmi, giochi ed altro. Se escludiamo le scuole specializzate, che tenevano, cioè, veri e propri corsi di Informatica, nelle altre non esistevano figure che svolgessero le funzioni di Sistemista o Analista o, per usare un termine generale, di Amministratore di tutto il sistema. Il responsabile di Laboratorio era semplicemente un volonteroso, o semplicemente chi, per sua fortuna (o sfortuna), ne sapeva un po' più degli altri e veniva, perciò, cooptato a svolgere le funzioni di suggerire acquisti a livello hardware e software, installare e disinstallare programmi, correggere i malfunzionamenti dovuti di solito ad operazioni errate, per lo più per colpa manifesta o per un atteggiamento che potremmo definire eufemisticamente incauto, da parte degli utenti. In altre parole, doveva fare sempre e in ogni modo da parafulmine quando qualcosa non funzionava.

I problemi della sicurezza implicavano essenzialmente due aspetti ... e mezzo.

1. la presenza di virus che entravano nei PC perché nascosti in file eseguibili memorizzati per lo più sui floppy-disk o sui CD-ROM. Era abbastanza raro trovare un PC con un antivirus aggiornato e in pratica nulla si sapeva dei firewall.

2. la cancellazione, volontaria o non, dei lavori eseguiti da altri studenti

3. il caos entropico delle icone sul Desktop, dove c'era di tutto, e dell'albero delle cartelle in cui venivano memorizzati i file con la lista numerosa di "Nuova cartella". Questo aspetto era meno importante dei primi due, ma creava in ogni caso confusione.

Era da poco apparso sul mercato Windows 95, ma quasi tutti a casa usavano ancora Windows 3.11. Come si sa, erano sistemi tutt'altro che sicuri e, soprattutto, monoutente. Volendo applicare alcuni criteri basilari di sicurezza quali, ad esempio, la conservazione sicura dei lavori salvati tra una lezione e l'altra, cercai una soluzione percorribile. A parte le alternative di altre ditte concorrenti della Microsoft (l'improponibile, per una scuola, Unix, il superiore ma elitario e più costoso sistema della Apple, lo sconosciuto Linux che stava movendo i primi passi) l'alternativa percorribile a quei tempi mi consigliò di appoggiarmi al neonato Windows NT 4 che era installato su un server posto in una stanza adiacente a quella del dirigente e che serviva solo per dare accesso alla rete esterna ai PC del laboratorio di Informatica. Infatti, era appena stato stipulato un contratto per la fornitura di accesso alla rete con un provider locale. Internet, magari con altra denominazione, era nata parecchi anni prima ma tra gli utenti singoli si stava diffondendo solo allora con l'esplosione del Web.

Mi rivolsi al responsabile del Laboratorio e gli chiesi di attivare 10 Utenti con relativa password in modo che i file venissero salvati sul server e solo l'utente specifico e l'Amministratore potessero accedervi. Ovviamente tenni una veloce e superficiale lezione introduttiva su alcuni concetti base, quali

l'architettura client-server, la rete locale, la sicurezza minima implementabile con il concetto di Account.

Mi ricordo che assegnai io stesso le password e feci in modo che fossero strane ma anche semplici da ricordare del tipo "AuSdRC,cO0,0" che sta semplicemente a significare "Assumo un sistema di riferimento cartesiano, con origine (nel punto) 0,0", usando le maiuscole per la parti principali del periodo (sostantivi, aggettivi, verbi) e le minuscole per le parti secondarie (articoli, congiunzioni, etc.). La cosa interessò e divertì nello stesso tempo. La soluzione, ancorché semplice, mi permise comunque di raggiungere l'obiettivo: attivare negli studenti il concetto di sicurezza seppur minima interessandoli ad un argomento che oggi, undici anni dopo, ha assunto proporzioni rilevanti per importanza al punto che ormai tutti almeno ne parlano.

Questa relazione non ha lo scopo di fare il punto della situazione sull'argomento "sicurezza" per la cui trattazione servirebbero corsi di settimane o mesi, ma vuole semplicemente focalizzarsi su un concetto particolare, quello della firma digitale, analizzando qualche aspetto legislativo.

Sarebbe velleitario anche voler trattare esaurientemente l'aspetto giuridico dell'argomento. Non sono un giurista, perciò non tratterò gli argomenti con pretesa di rigore dal punto di vista giuridico ma, anche se lo fossi, sono cosciente che mi dovrei muovere in una foresta intricatissima, almeno per quanto concerne il diritto italiano, fatta di Leggi, Regolamenti, Decreti Presidenziali, Decreti del Consiglio dei Ministri, Circolari, Norme Esecutive che si integrano e si sovrappongono continuamente.

Intendo trattare l'argomento dal punto di vista concettuale con i risvolti sociali implicati anche se sarà inevitabile la trattazione di argomenti tecnici.

Per raggiungere l'obiettivo analizzerò le leggi fondamentali che stanno alla base della firma digitale.

Le citazioni alla lettera, cioè le parti copia-incollate sono presentate in corsivo.

Estratto

La firma digitale nasce ufficialmente in Italia nel 1997 con la Legge n. 59 del 15 marzo 1997, che stabilisce che i documenti informatici sottoscritti con firma digitale sono equiparabili a quelli cartacei, dando il via ad una profonda innovazione, al punto che alcuni attori sono obbligati per legge ad utilizzare la rete per la trasmissione dei documenti previa autenticazione.

Il Decreto del Presidente della Repubblica n. 513 del 10 novembre 1997 fornisce le specifiche ed i requisiti che rendono informatico un documento e precisa le caratteristiche tecniche della firma digitale e del documento che devono essere protette e rese valide mediante crittografia a chiavi asimmetriche.

Il Decreto del Presidente del Consiglio dei Ministri dell'8 febbraio 1999 è senza dubbio la più importante legge in merito alla codifica dei documenti. Precisa meglio le caratteristiche tecniche della cifratura e della firma digitale e fornisce in pratica le direttive definitive del procedimento. Le norme approvate in seguito, infatti, non hanno fatto altro che apportare modifiche limitate anche se hanno complicato alquanto la procedura.

In seguito scende in campo (o sale in campo) anche la Comunità Europea con la Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999, con l'obiettivo di eliminare le divergenze delle norme degli Stati membri in materia di riconoscimento giuridico delle firme elettroniche e d'accreditamento dei prestatori di servizi di certificazione negli Stati membri.

Il Decreto Legislativo 23 gennaio 2002, n. 10 e il Decreto del Presidente della Repubblica del 7 aprile 2003, n. 137 modificano le disposizioni precedenti adeguandosi alla Direttiva CE e complicando la situazione. Si farà un breve cenno a questi Decreti.

Da ultimo sarà esaminato il Decreto Legislativo n. 82/2005 che, in pratica, apporta solo modifiche e correzioni.

Nascita della firma digitale

Legge n. 59 del 15 marzo 1997 - "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa"

Nell'anno odierno, A.D. 2007, o, se preferite, A. XXVII p. PC. n. (Anno ventisettesimo post Personal Computer natum) ricorre il decimo anniversario della nascita della firma digitale italiana. Risale, infatti, al **15 marzo del 1997 la Legge n. 59** che la introdusse in Italia: "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa".

In particolare l'art. 15, comma 2 precisa:

> *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.*

In pratica ciò equivale ad affermare che gli atti, i documenti di qualsiasi tipo, come i contratti di locazione o la denuncia dei redditi, elaborati con il PC o per via telematica e quindi sottoscritti con firma digitale, dalla Pubblica Amministrazione o dal cittadino comune, da allora in poi avrebbero assunto la stessa valenza di atti e documenti cartacei.

Questa innovazione fu molto importante ed aprì nuovi orizzonti fino a quel momento non considerati. È noto, infatti, ad esempio, che le denunce dei redditi vengono, in determinati casi, presentate per conto del dichiarante da parte di soggetti abilitati per via telematica direttamente all'Agenzia delle Entrate.

Scrive Marco Bellinazzo su "Il Sole-24 ore" del 15 marzo 2007 a dieci anni esatti dall'emanazione della legge in oggetto:

> *"La firma digitale è un fiore all'occhiello per l'Italia che è stato il primo Paese ad avere attribuito validità giuridica ai documenti elettronici."*

È importante rilevare che ciò era finalizzato, come recita l'art. 16,

> *alla modernizzazione delle pubbliche amministrazioni, all'efficacia e all'efficienza dei servizi pubblici nel quadro di una ottimizzazione e razionalizzazione dell'utilizzazione delle risorse finanziarie.*

Specifiche tecniche e definizioni

D.P.R. 10 novembre 1997, n. 513 - Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59

Naturalmente la legge, come accade sempre, dà direttive di carattere generale e non entra nel merito dei dettagli tecnici: quale sistema di crittografia applicare, quale Organizzazione od Ente è preposto al controllo o certificazione, la validazione temporale della firma, l'autenticazione della stessa, etc. Di solito, dopo qualche mese dall'approvazione della legge, viene emanato un Decreto, o del Presidente della Repubblica (d'ora in poi D.P.R.) o del Presidente del Consiglio dei Ministri (d'ora in poi D.P.C.M.) o di qualche altra autorità legislativa, che indica i criteri tecnici, le metodologie, gli strumenti e tutto ciò che serve per rendere esecutiva la legge appena approvata. A volte viene pubblicata una Circolare che spiega i contenuti poco chiari della legge e ciò capita di frequente.

Ed è ciò che è avvenuto con il successivo **D.P.R. 10 novembre 1997, n. 513**

In particolare il D.P.R. dà le definizioni tecniche di

documento informatico

firma digitale

sistema di validazione

chiavi asimmetriche

chiave privata

chiave pubblica

certificazione

validazione temporale

certificatore

revoca del certificato

sospensione del certificato

validità del certificato

Per non tediare troppo i "quattro lettori quattro" di questa relazione, non entro nel merito delle singole definizioni, poiché ritornerò su di esse nel seguito della relazione. Mi limito a ricordare i concetti principali.

L'art. 2 dà la definizione di documento informatico:

> *Il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento.*

Il successivo art. 5 è formato da due commi e stabilisce ciò che si debba intendere per efficacia probatoria del documento informatico:

> *1. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.*
>
> *2. Il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile e soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.*

In pratica, i duplicati, le copie, gli estratti del documento informatico e le copie su supporto informatico di documenti, formati in origine su supporto cartaceo sono validi e rilevanti a tutti gli effetti di legge se ad essi è apposta o associata la firma digitale di colui che li spedisce o rilascia.

Riporto il contenuto dell'art. 2702 del Codice Civile (d'ora in poi C.C.) perché suggerisce una considerazione interessante.

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

In pratica, la querela per falso può procedere sia nel caso di una scrittura privata di tipo cartaceo, ma anche nel caso di scrittura tramite un documento informatico purché sottoscritto con firma digitale secondo le disposizioni del D.P.R. in esame.

Come sappiamo, il C.C. è stato approvato nel 1942 ed i suoi articoli vengono ogni tanto modificati affinché siano coerenti con le mutate condizioni di vita sociale anche, e soprattutto, a seguito del progresso tecnologico. All'epoca in cui il C.C. è stato scritto l'Informatica era lontana anni luce, almeno da come la intendiamo oggi. Eppure l'art. 2702 non è cambiato rispetto alla stesura originale, semplicemente perché non è stato necessario alcun cambiamento. L'articolo si è automodificato ed autoadeguato in seguito all'art. 5 del D.P.R. che stiamo esaminando avendo questo introdotto il concetto di documento informatico ed avendolo equiparato ad una scrittura privata.

Sintetizzando, si raggiunge lo scopo di dare affidabilità ad un documento sottoscritto mediante firma digitale ascrivendolo, nello stesso tempo, ad un soggetto ben definito il quale, a sua volta, non può ripudiare il documento se lo ha sottoscritto esattamente com'è sempre avvenuto per una scrittura privata come affermato dal C.C.

Riprendendo in esame il D.P.R. 10 novembre 1997, n. 513, gli articoli seguenti si occupano della forma di cifratura, delle chiavi asimmetriche, della certificazione, degli obblighi dell'utente e del certificatore.

L'art. 10 entra nel merito tecnico della firma digitale.

> *1. A ciascun documento informatico, o a un gruppo di documenti informatici, nonché al duplicato o copia di essi, può essere apposta, o associata con separata evidenza informatica, una firma digitale.*
>
> *2. L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo.*
>
> *3. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.*

4. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa ad opera del soggetto pubblico o privato che l'ha certificata.

5. L'uso della firma digitale apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

6. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

7. Attraverso la firma digitale devono potersi rilevare, nei modi e con le tecniche definiti con il decreto di cui all'articolo 3, gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione.

Riassumendo quanto contenuto in questo articolo e nei seguenti si può affermare quanto segue.

La firma digitale è una forma di crittografia e questa serve a rendere comprensibili, leggibili, in una parola praticamente fruibili, determinati documenti crittografati, cioè camuffati opportunamente, solo a coloro che posseggono la chiave di lettura. In pratica si usano due chiavi asimmetriche, cioè diverse ma tra loro correlate e generate contemporaneamente con lo stesso algoritmo.

Le due chiavi sono una pubblica ed una privata. La prima è divulgata e resa disponibile a tutti. La seconda deve essere mantenuta segreta.

Il documento è codificato con una di esse e decifrato con l'altra. Non è possibile decodificare il documento con la stessa chiave con cui è stato crittografato. Per fare un esempio banale, se due persone posseggono ciascuna una mezza mappa di una zona in cui è sepolto un tesoro, nessuna delle due può sperare di poter trovare quanto spera se non con l'ausilio dell'altra mezza mappa che è in possesso dell'altro individuo.

La firma digitale serve principalmente a risolvere due problemi.

Innanzi tutto è possibile inviare un documento a tutti crittografandolo con la chiave privata. Applicando ad esso la chiave pubblica di chi lo ha inviato il documento verrà "aperto" da chiunque sia interessato a leggerlo e si avrà la certezza che esso sia stato inviato proprio dal mittente che lo ha firmato garantendo così l'autenticità della firma.

Se un documento, invece, è crittografato con la chiave pubblica del destinatario, esso potrà essere aperto solo con la chiave privata che è in possesso esclusivo dello stesso, rendendo il file prodotto inaccessibile a tutti gli altri.

Ulteriori specifiche tecniche

Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513

Il D.P.C.M. comprende tre soli brevi articoli ma l'allegato tecnico che lo accompagna (**Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513)** è molto corposo ed importante e si compone di ben 63 articoli, che analizzerò solo parzialmente.

Mi soffermo sui primi tre articoli del Titolo I (Regole tecniche di base). Innanzi tutto l'art. 1 conferma ed integra le definizioni stabilite nelle norme precedenti:

> *1. Ai fini delle presenti regole tecniche si applicano le definizioni contenute nell'art. 1 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513. S'intende, inoltre:*
>
> *per **"titolare"** di una coppia di chiavi asimmetriche, il soggetto a cui è attribuita la firma digitale generata con la chiave privata della coppia, ovvero il responsabile del servizio o della funzione che utilizza la firma mediante dispositivi automatici;*
>
> *per **"impronta"** di una sequenza di simboli binari, la sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;*
>
> *per **"funzione di hash"**, una funzione matematica che genera, a partire da una generica sequenza di simboli binari, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.*
>
> *per **"dispositivo di firma"**, un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali;*
>
> *per **"evidenza informatica"**, una sequenza di simboli binari che può essere elaborata da una procedura informatica;*
>
> *per **"marca temporale"**, un'evidenza informatica che consente la validazione temporale;*

Richiamo l'attenzione sul fatto che l'algoritmo di hash non è invertibile, in altre parole non è possibile ricostruire il documento a partire dal risultato finale dell'algoritmo stesso.

Inoltre, la stringa risultante è unica per ogni documento e perciò lo identifica univocamente marchiandolo indelebilmente. Al documento può essere applicata la firma digitale. Non solo: a partire da documenti diversi non è possibile ottenere la stessa stringa in uscita.

Il dispositivo di firma deve essere programmabile solo all'origine, deve, in pratica, contenere fin dal momento della sua creazione delle informazioni immodificabili successivamente.

I successivi due articoli stabiliscono che:

> ***Art. 2 - Algoritmi di generazione e verifica delle firme digitali***

1. Per la generazione e la verifica delle firme digitali possono essere utilizzati i seguenti algoritmi:

RSA (Rivest-Shamir-Adleman algorithm).

DSA (Digital Signature Algorithm).

Art. 3 - Algoritmi di hash

1. La generazione dell'impronta si effettua impiegando una delle seguenti funzioni di hash, definite nella norma ISO/IEC 10118-3:1998:

Dedicated Hash-Function 1, corrispondente alla funzione RIPEMD-160;

Dedicated Hash-Function 3, corrispondente alla funzione SHA-1.

Non entro nel merito della tecnica informatica degli argomenti, non essendo questo lo scopo di questa relazione e non andrò nemmeno ad esaminare la citata norma ISO/IEC.

L'art. 6 **(Modalità di generazione delle chiavi) stabilisce che**

1. La generazione delle chiavi di certificazione e marcatura temporale può essere effettuata esclusivamente dal responsabile del servizio che utilizzerà le chiavi.

2. Le chiavi di sottoscrizione possono essere generate dal titolare o dal certificatore.

3. La generazione delle chiavi di sottoscrizione effettuata autonomamente dal titolare deve avvenire all'interno del dispositivo di firma.

Ci sono dunque due modi per la generazione della coppia di chiavi. Il titolare stesso genera le chiavi e spedisce al certificatore la chiave pubblica. Il certificatore genera le chiavi e spedisce quella privata al titolare.

Il D.P.C.M. descrive poi le caratteristiche generali, la generazione e la conservazione delle chiavi. In particolare stabilisce

Art. 9 - Formato della firma

1. Le firme generate secondo le regole contenute nel presente decreto debbono essere conformi a norme emanate da enti riconosciuti a livello nazionale od internazionale ovvero a specifiche pubbliche (Publicly Available Specification – PAS).

2. Alla firma digitale deve essere allegato il certificato corrispondente alla chiave pubblica da utilizzare per la verifica.

Il TITOLO II del D.P.C.M. (Regole tecniche per la certificazione delle chiavi) dà indicazioni molto severe in merito all'elenco pubblico dei certificatori, alle caratteristiche ed al formato che devono possedere i certificati generati ed emessi dal certificatore, alla sospensione dei certificati su richiesta del titolare o di un terzo interessato, alla sostituzione della coppia di chiavi con richiesta presentata almeno 90 giorni prima della scadenza.

Le norme contenute in questo Titolo, che non espongo nei particolari, sono molto precise e molto severe al punto da rendere problematico l'inserimento nell'elenco pubblico di chi intendesse svolgere il ruolo di certificatore. A mio parere questo è un aspetto positivo perché, se da un lato può limitare il numero dei soggetti preposti alla certificazione, dall'altro lato dà garanzie sul soggetto che viene inserito nel registro pubblico e si è sottoposto ed ha superato tutti i severi controlli svolti dall'autorità pre-

posta allo scopo, il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), un tempo Autorità per l'informatica nella pubblica amministrazione (AIPA).

Di questo Titolo cito solo l'art. 26 che si occupa dell'eventuale personalizzazione del dispositivo di firma

> *1. La personalizzazione del dispositivo di firma consiste in:*
>
> > *acquisizione da parte del certificatore dei dati identificativi del dispositivo di firma utilizzato e loro associazione al titolare;*
> >
> > *registrazione, nel dispositivo di firma, dei dati identificativi del titolare presso il certificatore;*
> >
> > *registrazione, nel dispositivo di firma, dei certificati relativi alle chiavi di certificazione del certificatore.*
>
> *2. Durante la personalizzazione del dispositivo di firma il certificatore ne verifica il corretto funzionamento.*
>
> *3. La personalizzazione del dispositivo di firma è registrata nel giornale di controllo.*

Il titolo III (artt. da 52 a 61) si occupa delle Regole per la validazione temporale e per la protezione dei documenti informatici. In particolare si prescrive ciò che segue.

> ***Art. 52 - Validazione temporale***
>
> *1. Una evidenza informatica è sottoposta a validazione temporale con la generazione di una marca temporale che le si applichi.*
>
> *2. Le marche temporali sono generate da un apposito sistema elettronico sicuro in grado di:*
>
> > *mantenere la data e l'ora conformemente a quanto richiesto dal presente decreto;*
> >
> > *generare la struttura di dati contenente le informazioni specificate dall'articolo 53;*
> >
> > *sottoscrivere digitalmente la struttura di dati di cui alla lettera b).*

Il significato dell'art. 52 è abbastanza ovvio. Tutte le volte che sottoscriviamo un documento cartaceo qualsiasi, quale una lettera inviata ad un conoscente, il modulo di iscrizione all'Università, la richiesta di un bonifico bancario o quant'altro dobbiamo sempre firmare il documento e apporvi la data di richiesta o di presentazione. Ciò permette di dare al documento una veste giuridica. Se il documento è informatico deve valere la stessa regola.

Anche la marcatura temporale deve seguire rigidi criteri di sicurezza come dettato dagli articoli seguenti.

I titoli successivi IV e V si occupano delle regole tecniche per le pubbliche amministrazioni e delle disposizioni finali riguardanti le norme transitorie.

L'Europa si fa viva

Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999

Nei dieci anni di vita della firma digitale le cose sono mutate e sono andate complicandosi anche perché l'Italia ha dovuto adeguarsi ad alcune Direttive Europee. Esaminiamo brevemente la **Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 - Relativa ad un quadro comunitario per le firme elettroniche.**

Secondo il Parlamento Europeo ed il Consiglio dell'Unione Europea, le comunicazioni elettroniche e il commercio elettronico necessitavano di firme elettroniche e dei servizi ad esse relativi, atti a consentire l'autenticazione dei dati. Infatti, si preoccupavano, giustamente, della divergenza delle norme in materia di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione negli Stati membri e ciò poteva costituire un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico.

Al contrario, le suddette Istituzioni erano fiduciose che un quadro comunitario chiaro relativo alle condizioni applicate alle firme elettroniche avrebbe rafforzato la fiducia nelle nuove tecnologie e la loro accettazione generale nella convinzione che la normativa negli Stati membri non dovrebbe essere di ostacolo alla libera circolazione di beni e i servizi nel mercato interno.

È interessante esaminare l'art. 2 che dà importanti definizioni.

*1) "**firma elettronica**", dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione;*
*2) "**firma elettronica avanzata**", una firma elettronica che soddisfi i seguenti requisiti:*
essere connessa in maniera unica al firmatario;
essere idonea ad identificare il firmatario;
essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;
essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati;
*3) "**firmatario**", una persona che detiene un dispositivo per la creazione di una firma e agisce per conto proprio o per conto della persona fisica o giuridica o dell'entità che rappresenta;*
*4) "**dati per la creazione di una firma**", dati peculiari, come codici o chiavi crittografiche private, utilizzati dal firmatario per creare una firma elettronica;*
*5) "**dispositivo per la creazione di una firma**", un software configurato o un hardware usato per applicare i dati per la creazione di una firma;*
*6) "**dispositivo per la creazione di una firma sicura**", un dispositivo per la creazione di una firma che soddisfa i requisiti di cui all'allegato III;*
*7) "**dati per la verifica della firma**", dati, come codici o chiavi crittografiche pubbliche, utilizzati per verificare una firma elettronica;*
*8) "**dispositivo di verifica della firma**", un software configurato o un hardware usato per applicare i dati di verifica della firma;*
*9) "**certificato**", un attestato elettronico che collega i dati di verifica della firma ad una persona e conferma l'identità di tale persona;*
*10) "**certificato qualificato**", un certificato conforme ai requisiti di cui all'allegato I e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato II;*
*11) "**prestatore di servizi di certificazione**", un'entità o una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche;*

*12) "**prodotto di firma elettronica**", hardware o software, oppure i componenti pertinenti dei medesimi, destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica oppure per la creazione o la verifica di firme elettroniche;*
*13) "**accreditamento facoltativo**", qualsiasi permesso che stabilisca diritti ed obblighi specifici della fornitura di servizi di certificazione, il quale sia concesso, su richiesta del prestatore di servizi di certificazione interessato, dall'organismo pubblico o privato preposto all'elaborazione e alla sorveglianza del rispetto di tali diritti ed obblighi, fermo restando che il prestatore di servizi di certificazione non è autorizzato ad esercitare i diritti derivanti dal permesso fino a che non abbia ricevuto la decisione da parte dell'organismo.*

Viene introdotto il concetto di firma elettronica, che sono dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione;

È sicuramente una definizione molto meno forte di quella di firma digitale definita dalla normativa italiana come si è visto nel D.P.R. 10 novembre 1997, n. 513 e, soprattutto, nel Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999.

La successiva definizione di firma elettronica avanzata è molto migliore sul piano della sicurezza poiché permette di identificare il firmatario essendo connessa in maniera univoca ad esso. I mezzi, con cui la firma è creata, sono controllati in modo esclusivo dal soggetto firmante che può anche modificare i dati stessi.

In pratica, mentre la firma elettronica è implementata con qualsiasi mezzo idoneo all'autenticazione (pensiamo alla classica password, al codice PIN et similia), la firma elettronica avanzata è il risultato dell'applicazione di un algoritmo eseguito con mezzi informatici che permette l'identificazione ed autenticazione dei documenti informatici nonché del soggetto che li ha creati, cioè permette di identificare in modo univoco il firmatario garantendo anche l'evidenza di modifiche all'oggetto firmato, apportate dopo la sottoscrizione.

È importante anche il contenuto dell'art. 5 che si preoccupa di definire gli aspetti giuridici delle firme elettroniche e secondo il quale gli Stati membri avrebbero dovuto provvedere affinché, da quel momento, le firme elettroniche avanzate, basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura, possedessero i requisiti legali di una firma esattamente come una firma autografa li possiede per i dati cartacei.

Gli Stati membri avrebbero dovuto anche fare in modo che le firme elettroniche venissero ammesse come prova in giudizio.

In un articolo successivo veniva stabilito che entro il 19 luglio 2003 la Commissione avrebbe dovuto riesaminare l'applicazione della direttiva e presentare una relazione in merito al Parlamento europeo e al Consiglio.

È interessante notare che nel riesame si sarebbe dovuto valutare, tra l'altro, se l'ambito di applicazione della direttiva avrebbe dovuto essere modificato per tener conto dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici.

L'Italia si adegua (suo malgrado)

Decreto Legislativo 23 gennaio 2002, n. 10

D.P.R. del 7 aprile 2003, n. 137

A seguito della Direttiva 1999/93/CE l'Italia dovette adeguarsi ed emanare il **Decreto Legislativo** (d'ora in poi D.L.) **23 gennaio 2002, n. 10 - "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche",** mediante il quale andava a modificare in parte quanto stabilito dalle disposizioni di legge precedenti.

In particolare l'art. 2 ridefinisce alcuni concetti.

> *a) "**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;*
> *b) "**certificatori**" coloro che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi alle firme elettroniche;*
> *c) "**certificatori accreditati**" i certificatori accreditati in Italia ovvero in altri Stati membri dell'Unione europea, ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE;*
> *d) "**certificati elettronici**" gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità' dei titolari stessi;*
> *e) "**certificati qualificati**" i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti fissati dall'allegato II della medesima direttiva;*
> *f) "**dispositivo per la creazione di una firma sicura**" l'apparato strumentale, usato per la creazione di una firma elettronica, rispondente ai requisiti di cui all'articolo 10;*
> *g) "**firma elettronica avanzata**" la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, 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;*
> *h) "**accreditamento facoltativo**" il riconoscimento del possesso, da parte del certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza.*

Ritengo molto interessante quanto contenuto nell'art. 6 comma 5 che stabilisce che

> *Le disposizioni del presente articolo si applicano anche se la firma elettronica e' basata su di un certificato qualificato rilasciato da un certificatore stabilito in uno **Stato non facente parte dell'Unione europea**, quando ricorre una delle seguenti condizioni:*
> *a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed e' accreditato in uno Stato membro;*
> *b) il certificato qualificato e' garantito da un certificatore stabilito nella Comunità europea, in possesso dei requisiti di cui alla medesima direttiva;*
> *c) il certificato qualificato, o il certificatore, e' riconosciuto in forza di un accordo bilaterale o multilaterale tra la Comunità e Paesi terzi o organizzazioni internazionali.*

L'Italia si accorse che eravamo ormai in piena globalizzazione anche se il correttore ortografico della programma di scrittura che sto usando e che risale a quel periodo, anno più anno meno, si ostina a segnalarmi errore sul termine globalizzazione...

Il D.L. in esame stabilisce norme più rigide per i certificatori ed in particolare sui requisiti che devono possedere per essere ammessi al pubblico registro e sulla loro responsabilità.

Il comma 4 dell'art. 8 stabilisce quanto segue.

> *"4. La carta d'identita' elettronica e la carta nazionale dei servizi possono essere utilizzate ai fini dei pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalita' stabilite con decreto del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.*

Il successivo **D.P.R. del 7 aprile 2003, n. 137 (Regolamento recante disposizioni di coordinamento in materia di firme elettroniche ...)** interviene ancora ed apporta modifiche e qualche complicazione alle leggi precedenti il cui spirito rimane in sostanza invariato.

L'art. 1, tra le altre cose, introduce i seguenti concetti

> *c) **DOCUMENTO DI RICONOSCIMENTO** ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare;*
> *d) **DOCUMENTO D'IDENTITÀ** la carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare;*
> *e) **DOCUMENTO D'IDENTITÀ ELETTRONICO** il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età;*
> *n) **FIRMA DIGITALE** è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;*
> *cc) **FIRMA ELETTRONICA** ai sensi dell'articolo 2, comma 1, lettera a), del decreto legislativo 23 gennaio 2002, n. 10, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autentificazione informatica;*
> *dd) **FIRMA ELETTRONICA AVANZATA** ai sensi dell'articolo 2, comma 1, lettera g), del decreto legislativo 23 gennaio 2002, n. 10, la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, 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;*
> *ee) **FIRMA ELETTRONICA QUALIFICATA** la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;*

Mi piacerebbe fare un'inchiesta allo scopo di stabilire la media di carte elettroniche di cui siamo in possesso attualmente. Mi interrogo rapidamente e scopro che possiedo una decina di carte: carta d'identità, carta di credito, bancomat, carta regionale dei servizi, quattro carte per accumulare punti nei negozi di Tizio e di Caio e che serviranno per ricevere premi di scarsa utilità, due smart card per i due decoder e quanto prima anche la patente. E ancora: quante ne possiederemo in un futuro prossimo?

Inoltre, come si vede dalle definizioni, le firme sono ora diventate quattro. Evito di fare molti commenti perché, essendo "uomo di mondo", come diceva l'indimenticabile Totò, e non esperto di leggi, non riesco a capire la differenza tra firma digitale e firma elettronica qualificata. Almeno Wikipedia mi dà ragione poiché di esse dà un'unica definizione:

> *La **firma digitale**, o **firma elettronica qualificata, basata sulla tecnologia della crittografia a chiavi asimmetriche**, è un sistema di autenticazione di documenti digitali analogo alla firma autografa su carta.*

Altre definizioni (o altre complicazioni?)

Decreto Legislativo n. 82/2005

Come è logico aspettarsi l'art. 1 fornisce altre definizioni (o le stesse di prima complicate?)

Ai fini del presente codice si intende per:

*a) **allineamento dei dati**: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;*

*b) **autenticazione informatica**: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso;*

*c) **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;*

*d) **carta nazionale dei servizi**: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;*

*e) **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;*

*f) **certificato qualificato**: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;*

*g) **certificatore**: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;*

*h) **chiave privata**: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;*

*i) **chiave pubblica**: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;*

*l) **dato a conoscibilità limitata**: il dato la cui conoscibilità é riservata per legge o regolamento a specifici soggetti o categorie di soggetti;*

*m) **dato delle pubbliche amministrazioni**: il dato formato, o comunque trattato da una pubblica amministrazione;*

*n) **dato pubblico**: il dato conoscibile da chiunque;*

*o) **disponibilità**: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;*

*p) **documento informatico**: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;*

*q) **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;*

*r) **firma elettronica qualificata**: la firma elettronica ottenuta attraverso una procedura informatica che garantisce 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, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;*

*s) **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 al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;*

*t) **fruibilità di un dato**: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;*

*u) **gestione informatica dei documenti**: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;*

*v) **originali non unici**: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;*

*z) **pubbliche amministrazioni centrali**: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;*

*aa) **titolare**: la persona fisica cui é attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;*

*bb) **validazione temporale**: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.*

Non commento queste definizioni poiché, modifiche a parte, sono già state esaminate in precedenza. Rilevo solo che le firme da quattro sono diventate tre.

Più interessante è la lettura degli articoli 20 e 21 che esaminano il Documento informatico ed il suo valore probatorio una volta sottoscritto.

L'art. 20 afferma che il documento informatico, che era stato definito dalle leggi precedenti, la registrazione su supporto informatico e la trasmissione con strumenti telematici sono validi e rilevanti a tutti gli effetti di legge.

Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore e l'integrità del documento.

L'art. 21. (valore probatorio del documento informatico sottoscritto) prescrive che il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.

Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del C.C. (già esaminato all'inizio di questa relazione). L'utilizzo del dispositivo di firma permette di identificare il titolare.

Conclusioni

Pessimismo o ignoranza?

Scrive ancora Marco Bellinazzo, nell'articolo citato:

> *La firma digitale ha trasformato i rapporti tra i cittadini e la PA (Pubblica Amministrazione) e tra quelli tra privati. Ma, soprattutto, promette di imprimere un radicale mutamento alla gestione dei rapporti giuridici e finanziari nei prossimi anni.*
>
> *Già oggi è possibile pagare le imposte, presentando istanze e registrando atti per via telematica presso molte strutture pubbliche, compresi enti locali e realtà attivissime su questo fronte come le Camere di commercio.*
>
> *Ma non solo. Si sta rapidamente diffondendo – di pari passo con il moltiplicarsi delle firme digitali rilasciate dagli enti certificatori – l'abitudine a siglare contratti, emettere fatture o ordini d'acquisto online.*
>
> *L'espansione della firma digitale dipenderà molto però dalla semplificazione delle procedure ad essa connesse. Una semplificazione, che non pregiudichi la sicurezza.*

Plaudo all'ottimismo di Bellinazzo ma credo che ci sia ancora molto pessimismo e diffidenza nel cittadino comune. Non posso non considerare che molte persone che conosco sono ancora restie di fronte alla possibilità di fare acquisti in rete, anzi non li fanno per niente, adducendo come motivo che "non si fidano". Faccio sempre notare ai miei interlocutori che però non esitano ad affidare la carta di credito al cameriere oppure alla cassiera dell'ipermercato esponendosi ancor di più in fatto di sicurezza. Alla mia domanda non ottengo risposta.

Mi sono però fatto un'idea precisa. Chi diffida maggiormente sono, in generale, quelli che non esitano a scaricare programmi ed altro da qualunque sito e coloro che alla domanda "Quale firewall usi?" non sanno rispondere e quelli che accedono al proprio PC senza autenticazione perché si sono fatti installare il Sistema Operativo dall'amico e per comodità (o superficialità?) alla opzione che chiedeva di indicare se era necessaria la password per accedere al PC hanno risposto "No, tanto lo uso solo io".

Pessimismo = ignoranza, diffidenza, superficialità? credo di sì. Credo che costoro difficilmente si lasceranno coinvolgere nella possibilità di firmare digitalmente i loro documenti, ma posso sbagliarmi.

Ai posteri l'ardua sentenza.

Bibliografia

Letteratura

Marco Bellinazzo: Applicazioni (valida da 10 anni) – L'Italia resta all'avanguardia – Il Sole-24 Ore, 15 marzo 2007

Leggi e Decreti

Legge n. 59 del 15 marzo 1997

D.P.R. n. 513 del 10 novembre 1997

D.P.C.M. dell'8 febbraio 1999

Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999

D.L. 23 gennaio 2002, n. 10

D.P.R. del 7 aprile 2003, n. 137

D.L. n. 82/2005