

Firma elettronica e PEC

sabato 16 maggio 2009

Fino a qualche tempo fa i documenti inviati tramite computer avevano uno scarso valore giuridico, per questo motivo si è introdotta in Italia la cosiddetta firma digitale, cioè una firma elettronica apposta in base ad un sistema crittografico a chiave asimmetrica. Un documento dotato di firma digitale acquisisce valore di prova giuridica.

La firma digitale è definita come firma elettronica “forte”, laddove le firme elettroniche “deboli” sono le normali firme elettroniche che non danno certezza dell’individuo che invia la documentazione. Grazie alla partecipazione di un organismo esterno, detto certificatore, che accerta l’identità del soggetto, e rilascia i certificati che attestano tale identità, la firma digitale consente di avere la certezza giuridica dell’identità del soggetto che invia determinata documentazione tramite computer, in genere tramite mail.

La documentazione elettronica inviata con l’apposizione della firma digitale si considera esattamente uguale alla dichiarazione cartacea firmata a mano da chi la ha scritta, senza bisogno di doverla nemmeno stampare. Un giudice al quale si presenta tale tipo di documentazione la considererà valida dal punto di vista giuridico, quale prova dell’identità del soggetto da cui proviene. Il documento informatico sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata, fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l’ha sottoscritto.

La parte processuale contro la quale viene esibita in giudizio una falsa scrittura formata su supporto informatico con firma digitale, deve non solo disconoscere la propria firma, ma anche fornire le prove della sua falsità, con inversione dell’onere della prova.

La PEC, cioè la posta elettronica certificata è una applicazione della firma digitale, ed è stata resa obbligatoria con il Decreto Legge 185 del 2008, al precipuo scopo di darne lo stesso valore legale di una raccomandata con ricevuta di ritorno. In realtà la normativa prevede l’obbligatorietà di un indirizzo di posta certificata, basato su tecnologie che certifichino data e ora dell’invio e della ricezione delle comunicazioni e l’integrità del contenuto delle stesse, per cui la mail può essere sia di tipo PEC che di altro tipo.

Quando viene inviato un messaggio tramite posta elettronica certificata, il gestore del servizio del mittente invia allo stesso una ricevuta che costituirà valore legale dell’avvenuta o mancata trasmissione del messaggio, riportando l’indicazione temporale del momento in cui la mail è stata inviata. Allo stesso modo il gestore del destinatario fornirà al mittente altra ricevuta che attesti il momento dell’avvenuta consegna. In ogni caso sui server rimane per trenta mesi una traccia delle ricevute e del messaggio stesso.

Nel sito del CNIPA, il Centro Nazionale per l’Informatica nella Pubblica Amministrazione si trovano guide relative al funzionamento della PEC, le norme di riferimento e l’elenco dei gestori certificati.

Tornando alla normativa, essa prevede l’obbligo per società e professionisti di dotarsi di un sistema di certificazione della posta elettronica, cioè si è tenuti ad avere un indirizzo di posta elettronica certificata (cioè PEC) “o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell’invio e della ricezione delle comunicazioni e l’integrità del contenuto delle stesse, garantendo l’interoperabilità con analoghi sistemi internazionali”. Questo inciso è dovuto al fatto che la PEC è un sistema esclusivamente italiano, mentre nel resto del mondo si utilizzano sistemi differenti, in particolari i sistemi basati su certificati S/MIME (Secure Multipurpose Internet Mail Extensions), che consentono di autenticare e verificare l’integrità dei messaggi e ne garantiscono il “non ripudio” mediante l’utilizzo del certificato digitale. Inoltre applicano algoritmi di cifratura asimmetrica con chiave pubblica e privata.

Quindi il protocollo S/MIME, attraverso l’utilizzo di un certificato digitale, assolve a quanto previsto dall’articolo 16 comma 6 del DL 185/2008.

Ovviamente ci sono differenze tra i due sistemi, in particolare se si adotta la PEC si deve creare un nuovo account di posta elettronica presso uno dei gestori certificati, mentre adottando lo S/MIME si può continuare ad usare il proprio indirizzo di posta elettronica, scaricando l’apposito certificato (rilasciato dalla Certification Authority di riferimento) ed installandolo sul computer, consentendo quindi maggiore portabilità. Uno degli enti autorizzati ad emettere certificati S/MIME è, ad esempio, GlobalTrust, ma ovviamente ve ne sono altri. Una volta scaricato il certificato sarà possibile

utilizzarlo con la maggior parte dei client di posta elettronica (come Outlook, Thunderbird) e con le web mail (come Windows Live Mail e Google Mail).

GlobalTrust è certificatore italiano che rilascia un certificato gratuito con validità annuale, e rinnovabile, sempre gratuitamente. Visitando la pagina web si può richiedere un certificato che verrà rilasciato entro pochi giorni. Importante è svolgere tutta l'operazione, richiesta ed attivazione, con il medesimo browser (preferibile Firefox che ha una apposita estensione GMail_smime per gestire tali certificati in abbinamento con Gmail). Il certificatore, quindi, fornisce al richiedente il certificato, un numero di serie, la firma digitale e le informazioni per poter attivare ed utilizzare il certificato medesimo. Tutto ciò identifica il richiedente il certificato come unico possessore ed utilizzatore dello stesso.

Il certificato può essere salvato sull'hard disk al fine di impiegarlo con un client di posta elettronica. Dovrà essere salvato sotto forma di file con estensione .pfx. Ovviamente il file contiene anche la chiave privata, per cui non dovrà mai essere trasmesso a terzi. Per utilizzare il certificato con altri browser si dovrà esportarlo seguendo le istruzioni del browser specifico.

I pulsanti Codifica e Firma visualizzati in fase di composizione di un'e-mail permetteranno quindi di cifrare o firmare la mail che ci si appresta ad inviare.

Per usare il certificato S/MIME offerto da Globaltrust con Google Gmail, si dovrà importarlo in Mozilla Firefox accedendo al menù Strumenti, Opzioni, cliccando poi sulla scheda Avanzate e quindi su Cifratura e sul pulsante Mostra certificati. Dalla scheda Certificati personali si dovrà cliccare su Importa e selezionare il file .pfx relativo al proprio certificato S/MIME.