AWN – ArchiWorld Network

* * * * *

FD – Firma Digitale
PEC – Posta Elettronica Certificata

CARATTERISTICHE E FUNZIONALITÀ

Roma, rev. 1 – 13 marzo 2008

INDICE

N.B.: le informazioni relative alla FD sono tratte dalle *Linee guida per l'utilizzo delle Firma Digitale*, rilasciato dal CNIPA; quelle relative al alla PEC sul documento *Linee guida del servizio di trasmissione di documenti informatici mediante posta elettronica certificata*, rilasciato dal Centro Tecnico per la Rete unitaria della Pubblica Amministrazione e dal documento *La posta elettronica certificata* rilasciato dal CNIPA.

1. FD > Caratteristiche

1.1 Note generali

La firma digitale è uno strumento e come tale deve essere utilizzato nei modi e nei casi appropriati.

Ricordiamo che non è corretto il suo utilizzo come sistema di identificazione in rete, per il quale esistono strumenti quali la carta d'identità elettronica e le carte di accesso ai servizi.

La firma digitale è utile nel momento in cui è necessario sottoscrivere una dichiarazione ottenendo la garanzia di integrità dei dati oggetto della sottoscrizione e di autenticità delle informazioni relative al sottoscrittore.

La garanzia che il documento informatico, dopo la sottoscrizione, non possa essere modificato in alcun modo in quanto, durante la procedura di verifica, eventuali modifiche sarebbero riscontrate, la certezza che solo il titolare del certificato possa aver sottoscritto il documento perché non solo possiede il dispositivo di firma (smartcard/tokenUSB) necessario, ma è anche l'unico a conoscere il PIN (Personal Identification Number) necessario per utilizzare il dispositivo stesso, unite al ruolo del certificatore che garantisce la veridicità e la correttezza delle informazioni riportate nel certificato (dati anagrafici del titolare), forniscono allo strumento "firma digitale" caratteristiche tali da non consentire al sottoscrittore di disconoscere la propria firma digitale (fatta salva la possibilità di querela di falso).

Esempi tipici dell'utilizzo della firma digitale possono essere ricercati in tutti gli adempimenti da effettuarsi verso le amministrazioni che richiedono appunto la sottoscrizione di una volontà: denunce, dichiarazioni di cambi di residenza, di domicilio, richieste di contributi, di esenzioni a pagamenti a causa del reddito o di altre condizioni particolari, ricorsi, ecc.

Fra privati può trovare un interessante impiego nella **sottoscrizione di contratti**, **verbali di riunioni**, ordini di acquisto, **risposte a bandi di gara**, ecc.

Ancora, la firma digitale trova già da tempo applicazione **nel protocollo informatico, nella procedura di archiviazione documentale**, nel mandato informatico di pagamento, nei servizi camerali, nelle procedure telematiche d'acquisto, ecc.

1.2 La normativa di riferimento

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445
- Direttiva europea 1999/93/CE sulle firme elettroniche
- Centro Nazionale per l'Informatica nella Pubblica Amministrazione Area Regolazione
- Linee guida per l'utilizzo della Firma Digitale Pag. 5
- Decreto legislativo 23 gennaio 2002, n. 10
- Decreto del Presidente della Repubblica 7 aprile 2003, n. 137
- Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004

2. FD > Utilizzo

2.1 Il valore legale della Firma Digitale

La firma digitale ha trovato l'impianto legislativo necessario per il proprio utilizzo con la pubblicazione, in data 15 aprile 1999, delle regole tecniche costituite dal DPCM 8 febbraio 1999 (oggi sostituito dal DPCM 13 gennaio 2004).

In data 27 gennaio 2000 veniva incluso, nell'elenco pubblico dei certificatori, il primo soggetto autorizzato a rilasciare dispositivi di firma digitale utilizzabili per poter sottoscrivere documenti informatici con la medesima validità giuridica della firma autografa. Un richiamo ben preciso all'articolo 2702 del codice civile ne sanciva, infatti, la validità giuridica, prevedendo appunto che "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 è legalmente considerata come riconosciuta"

Quindi la firma digitale era giuridicamente valida, fatta salva la possibilità per il presunto sottoscrittore di disconoscerne la paternità. In tale evenienza era la controparte, e non il sottoscrittore, a doverne dimostrare la reale paternità.

Diversamente se una firma è "legalmente considerata come riconosciuta", ed è il caso ad esempio di una firma autenticata da un pubblico ufficiale, è il sottoscrittore che, per vederne nulli gli effetti, deve intentare una querela di falso.

Con il recepimento della Direttiva europea sulle firme elettroniche 1999/93/CE le cose sono cambiate.

Difatti, già il primo provvedimento legislativo, il DLGS 23 gennaio 2002, n.10, modificando l'articolo 10 (L) " Forma ed efficacia del documento informatico" del DPR 28 dicembre 2000, n.445 – dove era confluito il DPR 10 novembre 1997, n.513 – modificava, rafforzandolo, il valore giuridico di una sottoscrizione effettuata con firma digitale. Detto articolo, al comma 3, prescrive che " Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto "

Quindi, alla sottoscrizione con firma digitale "forte" (quella che possiede le seguenti caratteristiche: 1- è una firma elettronica avanzata, 2- è basata su un certificato qualificato, 3- è generata per mezzo di un dispositivo sicuro per la generazione delle firme) viene data la medesima validità giuridica di una **firma autografa autenticata da un pubblico ufficiale**.

A tutte le altre possibili tipologie di firme elettroniche, cioè quelle cui mancano uno o più delle tre caratteristiche indicate nel periodo precedente, viene esplicitamente conferito valore probatorio.

In un procedimento legale tali firme elettroniche dovranno essere di volta in volta analizzate dal giudice (che si avvarrà certamente di un perito) che deciderà se ammetterle quali prove in giudizio.

Questa previsione, che è stata resa esplicita per recepire senza dubbio alcuno quanto prescritto dalla Direttiva europea, era già presente nel nostro codice civile in quanto, lo stesso, prevede che nessuna prova in giudizio possa essere ricusata a priori.

2.2 Le procedure d'uso

Generare una firma digitale richiede la disponibilità del **kit di firma digitale** che, ricordiamo, è composto dal dispositivo sicuro di generazione della firme (smartcard o token), eventuale lettore di smartcard, software di firma in grado di utilizzare lo specifico dispositivo di cui si è dotati. Difatti, mentre è vero che è possibile verificare firme digitali generate utilizzando dispositivi eterogenei, non è possibile (salvo essere dotati di software disegnati a tale scopo) utilizzare dispositivi di firma forniti dal certificatore A con il software di firma fornito dal certificatore B.

La procedura di firma è piuttosto banale: dopo aver reso disponibile il dispositivo, inserendo quindi la smartcard nell'apposito lettore, l'applicazione di firma provvederà a richiedere l'inserimento del PIN di protezione, visualizzerà e richiederà di scegliere quale certificato si intende usare e procederà infine alla generazione della firma.

Ricordiamo infatti che un dispositivo sicuro di firma può contenere diversi certificati, e quindi diverse chiavi private, rilasciati per scopi diversi.

Tipico esempio potrebbe essere quello di un soggetto dotato di tre certificati di sottoscrizione: in qualità di cittadino, quale rappresentante legale di una società, quale componente di una commissione. Detto soggetto selezionerà, in fase di sottoscrizione, l'uno o l'altro certificato in dipendenza dalla natura dell'oggetto che si accinge a sottoscrivere.

La firma digitale di un singolo documento è operativamente dipendente dal software di firma di cui si dispone. Tale software può essere fornito da un certificatore, ma sono disponibili anche numerosi prodotti sviluppati da altre aziende.

Indipendentemente dal prodotto però i passi per la sottoscrizione digitale di un singolo documento sono sempre gli stessi.

- Bisogna ovviamente disporre di un personal computer al quale preventivamente sia stato collegato il lettore/scrittore di smart card in base alle indicazioni del fornitore.
- Dopo aver attivato il software di firma verrà richiesto di selezionare il documento da sottoscrivere e di inserire la smart card nel lettore se non lo si è ancora fatto. All'attivazione del processo di firma verrà richiesto di inserire il codice PIN della smart card e dopo qualche secondo potremo salvare un file sottoscritto e pronto per essere utilizzato.
- In base alla legislazione vigente sull'interoperabilità della firma digitale il file sottoscritto conserva il suo nome originale, al quale viene aggiunta l'estensione ".p7m". Ne risulta che il file **verbale.pdf**, dopo la sottoscrizione, diverrà **verbale.pdf.p7m** e come tale sarà fruito da altre applicazioni.

2.3 Le procedure di verifica

La procedura di verifica della firma digitale apposta ad un documento informatico consiste sostanzialmente nel verificare che:

1. il documento non sia stato modificato dopo la firma;
2. il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;
3. il certificato del sottoscrittore non sia scaduto;
4. il certificato del sottoscrittore non sia stato sospeso o revocato.

Per eseguire queste verifiche, oltre che per rendere leggibile il contenuto del documento, sono utilizzati specifici software. Detti software sono forniti dai certificatori ai titolari dei certificati;

coloro che non sono dotati di un kit di firma digitale possono altresì utilizzare dei software disponibili per uso personale a titolo gratuito: attualmente ne sono stati segnalati quattro, tre da installare sul proprio PC, il quarto disponibile via web. Detti software freeware sono stati resi disponibili dal CNIPA (Verifica_CT – www.cnipa.gov.it/), dalla Comped (DigitalSign – www.comped.it/), da Postecom (FirmaOK – www.poste.it/online/postecert), dalla società Digitaltrust (Sign'ncrypt – www.signncrypt.it) e da TrustItalia (Signo Reader – https://firmadigitale.trustitalia.it/).

Nel caso in cui si ritenga opportuno rendere pubblici, attraverso il proprio sito internet, dei documenti firmati digitalmente, si suggerisce di creare dei link a uno o più dei sistemi gratuiti di verifica sopra indicati.

Per eseguire la verifica non è necessario disporre di smartcard e lettore, in sintesi non si deve essere necessariamente dotati del kit di firma digitale.

Per eseguire le verifiche di cui ai punti 1, 2 e 3 è sufficiente essere dotati di un personal computer, di un prodotto utile per la verifica, piuttosto che del collegamento ad Internet per la verifica con il prodotto disponibile via web. Per la verifica al punto 4 è necessario avere accesso ad Internet. Difatti, i software di verifica si collegano alla lista di revoca dove il certificatore che ha emesso il certificato qualificato renderà disponibili le informazioni relative alla sospensione o revoca del certificato nel caso in cui si verifichi.

Per la verifica al punto 2 è necessario che sui software installati sul client siano stati caricati i certificati di certificazione dei soggetti iscritti nell'elenco pubblico.

A tale scopo, nel caso in cui i software forniti non abbiano già i certificati delle CA caricati, è necessario scaricare dal sito preposto l'elenco pubblico che contiene detti certificati e procedere alla loro installazione.

La procedura descritta è realizzabile in maniera completamente automatica, eventualmente con la necessità di disporre di una connessione a Internet per la verifica della revoca, che deve necessariamente basarsi su informazioni molto aggiornate, e quindi disponibili esclusivamente in rete. E' possibile, inoltre, che vi siano altre verifiche non effettuabili in modalità automatica.

In particolare, un certificato può avere dei limiti di validità dipendenti dalla natura del documento sottoscritto; a titolo di esempio, è possibile che un certificato qualificato garantisca la validità della firma a meno che essa non venga utilizzata per sottoscrivere contratti che coinvolgono transazioni monetarie che eccedono un limite stabilito dal certificatore. La firma di un contratto al di fuori di tali condizioni è considerata non valida, cioè corrisponde alla mancata sottoscrizione. Limiti di questo tipo non sono verificabili in maniera automatica, e richiedono all'utente di porre attenzione ad eventuali note che, comunque, sono sempre incluse nel certificato relativo alla firma che si sta verificando.

3. FD > Riferimenti e approfondimenti

- http://www.cnipa.gov.it/site/it-IT/
- http://www.cnipa.gov.it/site/_files/LineeGuidaFD_200405181.pdf
- http://www.interlex.it/docdigit/indice.htm

4. PEC > Caratteristiche

4.1 Note generali

Per posta elettronica certificata si intende un servizio basato sulla posta elettronica, come definito dallo standard SMTP e sue estensioni, che consenta la trasmissione di documenti prodotti mediante strumenti informatici nel rispetto dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

L'oggetto dell'invio fra mittente e destinatario è un messaggio di posta certificata composto dal messaggio originale, che coincide con quanto predisposto dal mittente, da una parte di testo descrittivo e dai dati di certificazione.

La trasmissione, tra mittente e destinatario, avviene mediante l'invio del messaggio di posta certificata sottoscritto dal gestore di riferimento del mittente con firma elettronica.

Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, i gestori devono mantenere traccia delle operazioni svolte su un apposito registro. I dati contenuti nel suddetto registro devono essere conservati per un periodo di almeno due anni e devono essere disponibili ed accessibili per la consultazione a fini ispettivi, da parte del Centro Tecnico, o in caso di contenzioso dai soggetti individuati per tale compito. Per la gestione del registro i gestori devono adottare le soluzioni tecniche e organizzative che garantiscano la riservatezza e la sicurezza (autenticità ed inalterabilità nel tempo) delle informazioni in esso contenute.

Nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi inviati, le informazioni presenti nei registri degli operatori coinvolti nell'invio sono opponibili ai terzi ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

4.2 La normativa di riferimento

- DPR del 11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3" (G.U. del 28 aprile 2005, n. 97);
- Decreto Ministeriale del 2 novembre 2005, "Regole tecniche per la formazioni, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (G.U. del 14 novembre 2005, n. 265);
- Circolare CNIPA CR/49 del 24 novembre 2005, "Modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata" (G.U. del 5 dicembre 2005, n. 283);
- D. Lgs. del 7 marzo 2005, n. 82 (G.U. del 16 maggio 2005, n. 93), "Codice dell'amministrazione digitale".

5. PEC > Come funziona

Gli attori coinvolti nel processo di gestione della PEC sono:

- l'utente mittente, cioè il soggetto che ha l'esigenza di inviare un documento informatico;
- l'utente destinatario, il soggetto al quale sarà destinato l'oggetto dell'invio;

- il gestore del mittente, il soggetto con il quale il mittente mantiene un rapporto finalizzato alla disponibilità del servizio di PEC;
- il gestore del destinatario, il soggetto con il quale il destinatario mantiene un rapporto finalizzato alla disponibilità del servizio di PEC;
- la rete di comunicazione, che tipicamente può essere considerata internet;
- il documento informatico, realizzato dal mittente ed oggetto dell'invio verso il destinatario.

Sia il mittente che il destinatario devono disporre di un PC (o altro idoneo dispositivo) e della connessione al proprio gestore di PEC. Di seguito si considererà il caso più generale che prevede che il mittente ed il destinatario facciano riferimento a due gestori diversi; le successive considerazioni valgono comunque anche nel caso in cui mittente e destinatario facciano riferimento ad uno stesso gestore.

Il punto di partenza del processo coinvolge il mittente che con i propri strumenti predispone uno o più documenti informatici; è bene ricordare che la PEC è un servizio di trasporto ed in quanto tale non entra nel merito di ciò che è oggetto del trasferimento dal mittente al destinatario. Quindi il mittente, con la PEC, può inviare qualsiasi tipo di documento informatico, ad esempio un testo, un'immagine, un programma e così via.

Predisposto l'oggetto dell'invio, il mittente, si deve far riconoscere dal sistema di PEC del proprio gestore secondo le modalità da questi previste. Una modalità che potrà trovare ampia diffusione sarà ad esempio la classica accoppiata user-id/password; ciò non toglie la possibilità di adottare modalità diverse e con maggiori livelli di sicurezza quali, ad esempio, le smart card.

Superata la fase di riconoscimento, il mittente, utilizzando l'interfaccia disponibile, che verosimilmente sarà il classico client di posta elettronica o in alternativa un web browser, predispone il messaggio di PEC e quindi lo invia. È bene evidenziare che il mittente opererà secondo le abituali modalità previste per l'invio di un messaggio di posta elettronica convenzionale.

A seguito dell'invio, il sistema di PEC del mittente effettua una serie di controlli inalizzati a verificare la correttezza formale del messaggio e l'assenza di virus. Nel caso i controlli evidenziassero delle criticità il messaggio non verrebbe inoltrato verso il destinatario ed il mittente riceverebbe una ricevuta, firmata elettronicamente dal proprio gestore di PEC, contenente l'informazione che l'invio non ha avuto luogo e le relative motivazioni.

Qualora i controlli, realizzati in fase di invio, non rilevino criticità il gestore mittente provvede ad inserire, come allegato, il messaggio preparato dal mittente ed a firmarlo digitalmente. Quest'ultima operazione è finalizzata a garantire l'inalterabilità del messaggio che il mittente ha predisposto per l'invio.

A questo punto, il gestore mittente provvede ad inoltrare tramite la rete il messaggio verso il gestore destinatario.

Quest'ultimo, ricevendo ciò che è stato inoltrato dal gestore mittente, provvede ad effettuare una serie di verifiche finalizzate a controllare la provenienza (da un gestore PEC iscritto nell'apposito elenco) e l'integrità del messaggio ricevuto. Questi ultimi controlli sono finalizzati ad avere tutte le garanzie in merito alla non alterazione del messaggio nel suo transito tra un gestore ed un altro.

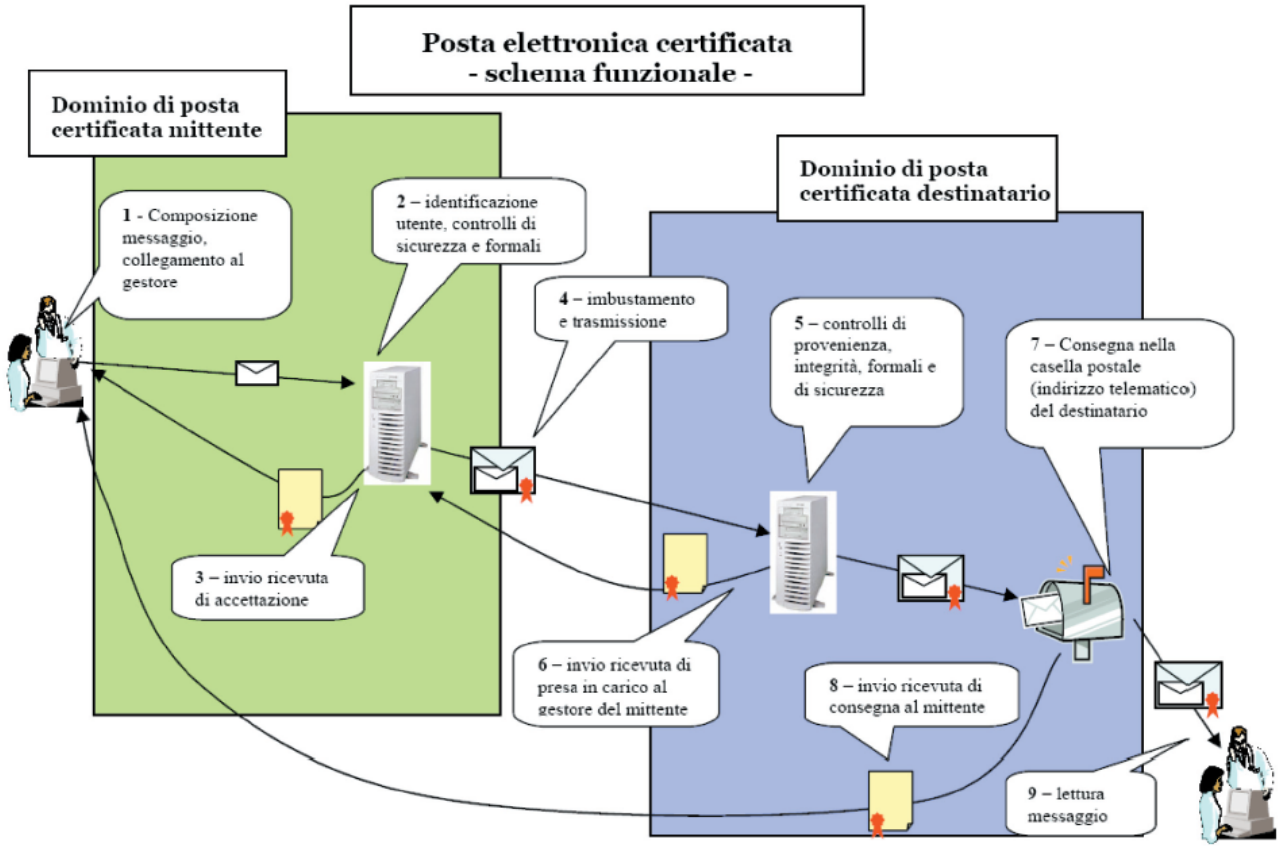
Fra i controlli effettuati, anche in questo caso si rileva l'eventuale presenza di virus che bloccherebbero l'inoltro del messaggio verso il destinatario.

Questa situazione comporta una notifica, al mittente, di mancata consegna del messaggio inviato per problemi di sicurezza.

Il gestore destinatario, quindi, procede a depositare il messaggio nella casella del destinatario. A conclusione di questa operazione, il gestore destinatario provvede ad inviare la ricevuta di avvenuta consegna al mittente. Tale ricevuta attesta che il messaggio inviato dal mittente è stato depositato nella casella del destinatario (indirizzo telematico da questi prescelto) ed inoltre può evidenziare anche il contenuto dell'invio (una delle opzioni prevede nella ricevuta l'intero messaggio inviato). Anche in questo caso la ricevuta di avvenuta consegna è firmata elettronicamente dal gestore destinatario al fine di garantire la validità giuridica della stessa nei casi di utilizzo.

Il destinatario appena ha disponibile nella sua casella il messaggio ricevuto, i norma riceve dal sistema di posta elettronica una notifica dell'evento e quindi può accedere il messaggio per la lettura (da notare che si tratta di una prestazione dei sistemi di posta elettronica sui quali si basa la PEC e non dei sistemi PEC). È importante evidenziare, che il sistema di PEC, essendo un sistema di trasporto, non considera la lettura del messaggio poiché è un'azione successiva al completamento del processo di trasporto del messaggio, coerentemente con il fatto che il messaggio consegnato all'indirizzo telematico prescelto dal destinatario si intende nella disponibilità di quest'ultimo esattamente quando viene depositato nella relativa casella PEC che corrisponde al predetto indirizzo.

Nelle due situazioni di invio e ricezione laddove il gestore rilevi la presenza di virus nel messaggio, non deve trasmetterlo e deve mantenere il messaggio in un apposito archivio per una durata di trenta mesi, così come previsto dalle norme, al fine di poter effettuare successive verifiche circa l'evento rilevato.



6. PEC > Riferimenti e approfondimenti

- http://www.cnipa.gov.it/site/_files/Interno%2011.pdf
- http://www.interlex.it/testi/pdf/postcert_lg.pdf