

**RIASSUNTO DEL CONVEGNO SULLA POSTA  
ELETTRONICA CERTIFICATA E LA FIRMA DIGITALE  
TRIESTE 3 FEBBRAIO 2011**

**a cura dell'Avv. Stefano Corsini**

PEC è l'acronimo di Posta Elettronica Certificata. E' un sistema che consente l'invio di messaggi e-mail conferendo valore legale al processo di consegna dei messaggi, essendo fornita al mittente l'attestazione elettronica dell'invio e della consegna di messaggi e dei loro eventuali allegati.

Ciò che rende la trasmissione PEC valida agli effetti di legge, sono le ricevute elettroniche che i gestori PEC emettono, "certificando" l'avvenuto invio di un documento informatico da parte del mittente, l'avvenuta ricezione dello stesso documento da parte del destinatario e i riferimenti temporali della trasmissione.

La PEC è utile e valida per spedire documenti e messaggi utilizzando i vantaggi e le funzionalità della posta elettronica, con l'aggiunta di una certificazione di invio, quindi in termini di opponibilità in giudizio, una documentazione certa (esattamente come per una Raccomandata Postale).

E' 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, ma in ogni caso la PEC non dà all'allegato alcun valore di documento firmato digitalmente ai sensi dell'art. 21 del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale). Si precisa sin d'ora che PEC e firma digitale sono due strumenti separati ed indipendenti, che tuttavia possono essere utilizzati congiuntamente in determinate ipotesi.

La Legge 2/2009 ha reso obbligatoria per alcuni soggetti (pubblica amministrazione, imprese in forma societaria, professionisti iscritti in albi) la comunicazione del proprio indirizzo PEC con scadenze e modalità differenti per i diversi soggetti (per i professionisti da novembre 2009, per le nuove imprese da novembre 2008; le imprese già esistenti dovranno assolvere tale obbligo entro novembre 2011).

La consultazione per via telematica dei singoli indirizzi di posta elettronica certificata nel registro delle imprese o negli albi o elenchi costituiti avviene liberamente e senza oneri.

Per sapere gli indirizzi di PEC delle P.A. è possibile consultare i siti [www.indicepa.gov.it](http://www.indicepa.gov.it) oppure il più recente [www.paginepecpa.gov.it](http://www.paginepecpa.gov.it).

La previsione contenuta nella legge n. 2 del 2009 si applica a tutte le professioni regolamentate per le quali il legislatore abbia prescritto la tenuta di un albo o elenco.

I professionisti non possono utilizzare la casella di PEC gratuita per i cittadini per l'esercizio della loro attività. La PEC gratuita viene infatti attribuita solo ai cittadini richiedenti per semplificare i rapporti con la P.A., riducendo tempi e costi delle comunicazioni.

L'obbligo posto a carico dei professionisti è invece finalizzato a migliorare le comunicazioni fra la P.A. e soggetti che operano sul mercato in qualità di esercenti una libera professione.

I professionisti, dipendenti delle P.A. iscritti nei rispettivi albi o in apposite sezioni separate degli stessi, debbono dotarsi di una casella di PEC indipendentemente dal possesso di quella eventualmente fornita dal datore di lavoro.

Nella L. 2/2009 non è prevista alcuna sanzione diretta verso i professionisti che non si sono dotati di casella PEC, tuttavia le sanzioni saranno stabilite dagli Ordini, i quali hanno l'obbligo di controllare il rispetto della normativa da parte dei loro iscritti (per verificare il rispetto degli adempimenti prescritti per gli Ordini o Collegi Professionali, il Ministro per la pubblica amministrazione e l'innovazione ha recentemente incaricato l'Ispettorato per la funzione pubblica di avviare gli opportuni accertamenti).

In uno studio associato ogni professionista deve dotarsi della sua casella personale di PEC, ad esempio utilizzando quella fornita tramite l'Ordine di appartenenza, mentre lo studio, inteso come persona giuridica, deve dotarsi di un'ulteriore casella di PEC entro la fine di novembre 2011.

Il funzionamento è molto semplice: il mittente PEC scrive il suo messaggio PEC dal proprio indirizzo e-mail PEC e lo invia al suo destinatario; attraverso la trasmissione sicura il messaggio viene ricevuto dal server di posta del Gestore PEC; questi ne dà ricevuta certificata al mittente. A questo punto il Gestore PEC del mittente prende in carico il messaggio sigillandolo in una "busta elettronica" e lo spedisce al server di posta del Gestore PEC del destinatario, il quale prende in carico il messaggio e lo consegna nella casella e-mail del destinatario, dandone ricevuta certificata al mittente. I due messaggi di conferma che vengono spediti al mittente sono i due certificati di trasmissione validi a norma di legge, poiché testimoniano l'avvenuta trasmissione del messaggio e i tempi in cui essa è avvenuta.

Potrà essere usata in alternativa ad altre forme di comunicazione con valore legale (come le Raccomandate con ricevuta di ritorno), direttamente dal proprio computer, o via web, senza doversi recare fisicamente in un ufficio postale.

La disponibilità da parte del mittente della ricevuta di avvenuta consegna non garantisce la lettura del messaggio da parte del destinatario, è solo la certificazione che il messaggio spedito, eventualmente contenente allegati, è stato consegnato - inalterato - nella casella di Posta Elettronica Certificata del destinatario. Il destinatario di un messaggio di PEC non può negarne l'avvenuta ricezione.

Può essere quindi utilizzata da chiunque abbia bisogno di uno strumento di comunicazione ufficiale e certo:

- privati, in alternativa alle raccomandate A/R postali
- aziende/professionisti, nell'espletamento delle loro funzioni: interne (convocazioni, trasmissione documenti, ecc.), verso clienti (invio fatture, contratti), verso la pubblica amministrazione (istanze, tributi, fatture)
- enti pubblici nei rapporti con i propri utenti/iscritti, per l'invio di materiale fiscale, comunicazioni, richieste, ecc.
- pubblica amministrazione nell'espletamento delle proprie funzioni istituzionali, nei rapporti con cittadini, professionisti e aziende.

I punti di forza della Posta Elettronica Certificata sono:

Velocità. Al pari di una qualsiasi comunicazione via e-mail, la trasmissione dei messaggi PEC è immediata, diversamente dalla raccomandata a/r che ha i suoi tempi "tecnici" (in particolare la cartolina di ricezione).

Economicità. Si risparmiano i costi in termini di tempo e denaro di una classica raccomandata a/r (spedizione, parcheggio, tempo impiegato, ecc.).

Certificazione. Ha lo stesso grado di certificazione di una raccomandata postale, relativamente a data e ora della trasmissione.

Valore legale. Come una raccomandata ha valore legale, opponibile a terzi in giudizio.

Sicurezza. I gestori di posta elettronica certificata trasmettono il messaggio di posta elettronica certificata dal mittente al destinatario integro in tutte le sue parti, includendolo nella busta di trasporto. I gestori hanno l'obbligo di mantenere per 30 mesi le ricevute di consegna e accettazione, con soluzioni tecniche che ne garantiscano la sicurezza e l'inalterabilità nel tempo.

Antivirus. Qualora i gestori PEC ricevano messaggi contenenti virus, a differenza dei fornitori tradizionali di servizi e-mail (libero/virgilio, ecc.), effettuano un approfondito controllo antivirus e provvederanno a bloccare l'invio dei messaggi e ad informare il mittente di tali messaggi dell'impossibilità di trasmetterli. Il gestore PEC del mittente, che riceve virus dal mittente, informerà lo stesso mittente. Il gestore pec del destinatario che eventualmente ricevesse un messaggio contenente virus dal gestore pec del mittente, informerà il gestore pec del mittente.

Inalterabilità. La trasmissione avviene in presenza di protocolli di sicurezza che garantiscono che il messaggio non venga alterato durante il suo percorso da mittente a destinatario. I gestori di posta elettronica certificata trasmettono il messaggio di posta elettronica certificata dal mittente al destinatario integro in tutte le sue parti, includendolo nella busta di trasporto.

Ciò che rende la trasmissione PEC valida agli effetti di legge, sono le ricevute elettroniche che i Gestori PEC emettono, “certificando”:

- l’avvenuto invio di un documento informatico da parte del mittente;
- l’avvenuta ricezione dello stesso documento da parte del destinatario;
- i riferimenti temporali della trasmissione (si dimostra di aver effettuato un’operazione in una data ora in un dato giorno).

Nella compilazione del messaggio, gli indirizzi PEC di destinazione possono essere inseriti sia nel campo "A..." / "To..." sia nel campo "Copia Conoscenza" / "Cc..."

Non si può spedire via PEC ai destinatari contenuti nei campi "Copia Conoscenza Nascosta" / "Ccn.." / "Bcc..."

È importante sottolineare che il servizio di Posta Elettronica Certificata è “completo”, ovvero produce le certificazioni – a valore legale – attestanti l’invio e la consegna di un messaggio, solo se entrambi gli interlocutori dispongono di caselle PEC, anche facenti capo a Gestori diversi (dovendo i vari Gestori garantire l’interoperabilità dei servizi offerti).

Contrariamente, qualora da una casella di PEC si spedisca un messaggio ad un destinatario che non ha una casella di posta certificata, l’unica ricevuta prodotta dal sistema è quella di accettazione, proveniente dal Gestore del mittente. Infine, qualora un messaggio di posta elettronica ordinaria venga spedito ad un destinatario PEC possono presentarsi due distinte situazioni: il messaggio non viene accettato dal Gestore e quindi non arriva al destinatario, ovvero il messaggio entra nel sistema PEC e giunge al destinatario all’interno di una busta di anomalia (per maggiori dettagli si rimanda alle Regole Tecniche allegate al D.M. 2 novembre 2005). I criteri per la gestione della posta elettronica ordinaria sono a discrezione del Gestore (che deve comunque comunicarli ai propri utenti) il quale potrebbe decidere, ad esempio per limitare il dannoso fenomeno dello spam, di non accettare messaggi provenienti da domini non PEC.

Configurando la propria casella PEC è poi possibile far sì che i messaggi standard in entrata vengano automaticamente reindirizzati ad un altro indirizzo standard, oppure è possibile impostare la comunicazione automatica al proprio indirizzo standard in caso di ricevimento di una PEC nella nostra casella certificata (opzione consigliata in particolare in questa fase di avvio dell’utilizzo di PEC).

È possibile ricevere e spedire messaggi dal proprio client di posta (Outlook, Thunderbird, ecc.), configurando un nuovo account di posta certificata. Bisognerà tuttavia impostare una configurazione particolare per l’indirizzo PEC (operazione facile seguendo le istruzioni del fornitore).

Per chi invece non usa tali software, la casella PEC è comunque accessibile attraverso il sito web di riferimento (cd. webmail: <https://webmail.archiworldpec.it/index.html?customer=default>).

A partire dal 1997, una serie di provvedimenti legislativi hanno conferito valore giuridico al documento informatico e alla firma digitale.

Il primo atto normativo che ha stabilito la validità della firma digitale per la sottoscrizione dei documenti elettronici è stato il D.P.R. 10 novembre 1997 n. 513 (regolamento recante criteri e modalità per la formazione, l’archiviazione e la trasmissione di documenti con strumenti informatici e telematici), emanato in attuazione dell’articolo 15 della legge 15 marzo 1997, n. 59.

Successivamente, tale normativa è stata trasposta nel D.P.R. 28 dicembre 2000 n. 445 (il T.U. sulla documentazione amministrativa), più volte modificato negli anni successivi all’emanazione, per conformare la disciplina italiana alla normativa comunitaria contenuta nella Direttiva 99/93 in materia di firme elettroniche. Oggi, la legge che disciplina la firma digitale è il “**Codice dell’amministrazione digitale**” (Decreto Legislativo 7 marzo 2005, n. 82, così come modificato dal D.Lgs. n. 235/2010). Il

Codice, all'articolo 1, distingue i concetti di firma elettronica, firma elettronica avanzata, firma elettronica qualificata e firma digitale.

a) Per “firma elettronica” la legge intende l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

b) per “firma elettronica avanzata”: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

c) per “firma elettronica qualificata”: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

d) per “**firma digitale**” (attualmente quella più diffusa in Italia: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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;

Il D.Lgs. 82/2005, quindi, è impostato come se si potessero avere più tipi di firma elettronica, ossia più sistemi che consentano l'identificazione univoca del titolare, uno solo dei quali è la firma digitale a chiavi asimmetriche. Di fatto, però, nella realtà concreta, la firma digitale è l'unico tipo di firma elettronica qualificata oggi conosciuto e utilizzato, per cui i due concetti tendono a coincidere. La distinzione è stata fatta per non precludere al nostro Paese l'interoperabilità con altri sistemi extranazionali.

Il D.Lgs. 82/2005 stabilisce, con un rimando all'art. 2702 del Codice Civile, che la firma digitale (e la firma elettronica qualificata e avanzata) **fa piena prova fino a querela di falso** se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta, equiparando così il documento informatico sottoscritto con firma digitale alla scrittura privata sottoscritta con firma autografa (e non, come avveniva in precedenza, alla scrittura privata con firma autenticata). Tuttavia vi è una significativa differenza tra firma autografa e firma digitale rispetto alla procedura di disconoscimento. Nel primo caso infatti è sufficiente che il convenuto avvii una formale istanza di disconoscimento senza doversi assumere alcun onere probatorio. Nel secondo caso (firma digitale), l'articolo 21 stabilisce che l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria. Vi è quindi un'inversione dell'onere della prova dall'attore verso il convenuto. Sulla questione del valore probatorio del documento informatico c'è stata in Italia una lunga discussione che è sfociata in modifiche normative contraddittorie.

La titolarità della firma digitale è garantita dai “certificatori” (disciplinati dagli articoli 26-32): si tratta di soggetti con particolari requisiti di onorabilità, che possono essere accreditati presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA, ora DigitPA), che tengono registri delle chiavi pubbliche, presso i quali è possibile verificare la titolarità del firmatario di un documento elettronico. Fra le caratteristiche per svolgere l'attività di certificatore di firma digitale vi è quella per cui occorre essere una società con capitale sociale non inferiore a quello richiesto per svolgere l'attività bancaria. I certificatori non sono quindi soggetti singoli (come i notai), ma piuttosto grosse società (per esempio, certificatori sono la società Postecom oppure Infocert).

Concludendo, possiamo dire che nell'utilizzo del documento informatico, quando si ha la necessità di una sottoscrizione equivalente a quella autografa è indispensabile utilizzare la firma digitale.

Negli altri casi possiamo tranquillamente affermare che più che di un processo di firma si tratta di un processo di autenticazione o identificazione, con minori requisiti di sicurezza e quindi con una minore efficacia probatoria.

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* o *dispositivo USB*) necessario, ma è anche l'unico a conoscere il PIN per utilizzare il dispositivo stesso, unite al ruolo del certificatore che garantisce la veridicità e la correttezza delle informazioni riportate nel certificato, forniscono al questo strumento caratteristiche tali da non consentire al sottoscrittore di disconoscere la propria firma digitale.

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, istanze di accesso, ecc.

Fra privati può trovare un interessante impiego nella sottoscrizione di offerte e contratti, progetti, verbali di riunioni, perizie, risposte a bandi di gara, ecc.

E' possibile anche attribuire al documento firmato digitalmente una "data certa", attraverso l'utilizzo della cd. "**marca temporale**". Così facendo - il servizio è a pagamento - sarà possibile datare con validità ai fini di legge tutti i documenti che la richiedono.

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 e nelle sperimentazioni del processo civile telematico.

Avv. Stefano Corsini