Contenuti tecnici dei sistemi di Posta Elettronica Certificata e Firma Digitale

Premesse e informazioni

Il D.L. 185/2008, converito in Legge n. 2 del 28 gennaio 2009, all'art. 16, commi. da 6 a 10, ha previsto per le imprese costituite in forma societaria, per i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato, nonché per le amministrazioni pubbliche, l'obbligo di istituire un indirizzo di posta elettronica certificata entro il 29 novembre 2009 ed ha stabilito che Ordini e Collegi debbano pubblicare in un elenco consultabile in via telematica **esclusivamente** dalle pubbliche amministrazioni, i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata.

Contenuti del sistema di Posta Elettronica Certificata (PEC)

La (PEC) è uno strumento che, grazie all'uso di tecnologie crittografate, permette di dare ad un messaggio di posta elettronica un valore equivalente a quello di una raccomandata; nel caso sia inviata a un altro indirizzo di posta certificata ha anche il valore equivalente di una raccomandata con ricevuta di ritorno tradizionale.

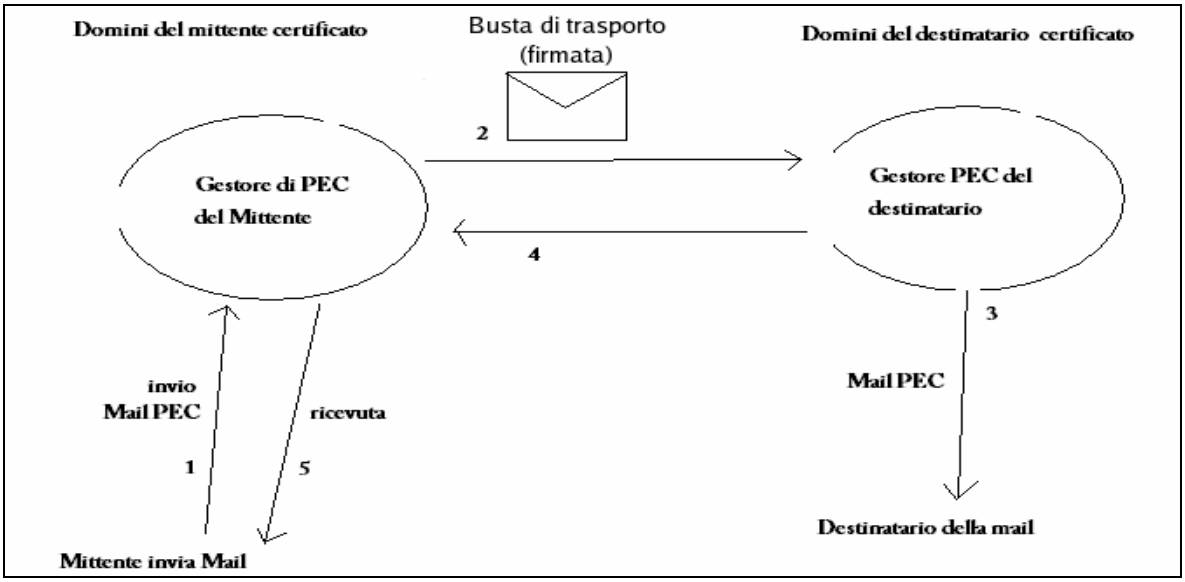
Al momento dell'invio di una mail PEC il gestore PEC del mittente si occuperà di inviare al mittente una ricevuta che costituirà valore legale dell'avvenuta (o mancata) trasmissione del messaggio con precisa indicazione temporale del momento in cui la mail PEC è stata inviata. In egual modo il gestore del destinatario, nel caso di tratti di invio a una casella di posta certificata, dopo aver depositato il messaggio PEC nella casella PEC del destinatario, fornirà al mittente una ricevuta di avvenuta consegna, con l'indicazione del momento temporale nel quale tale consegna è avvenuta.

In caso di smarrimento di una delle ricevute presenti nel sistema PEC è possibile disporre, presso i gestori del servizio, di una traccia informatica avente lo stesso valore legale in termini di invio e ricezione, per un periodo di trenta mesi, secondo quanto previsto dall'art. 11 del D.P.R. 68/2005.

Dal punto di vista dell'utente, una casella di posta elettronica certificata non si differenzia da una casella di posta normale: cambia il meccanismo di comunicazione sul quale si basa la PEC e che si fonda sulle ricevute inviate dai gestori PEC a mittente e destinatario. La PEC garantisce la certificazione del contenuto del messaggio e, assicurando l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge (*art. 14, comma 3 DPR 445/2000*).

Il funzionamento di un sistema di PEC è descritto nella figura sottostante.

In questo caso i messaggi di posta certificata vengono spediti tra 2 caselle mail certificate.



Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato (passo 1), il messaggio viene raccolto dal Gestore del dominio certificato (punto di accesso) che lo racchiude in una busta di trasporto e vi applica una firma elettronica in modo da garantire inalterabilità e provenienza.
Fatto questo, indirizza il messaggio al Gestore di PEC destinatario (passo 2, punto di ricezione) che verifica la firma e lo consegna al destinatario (passo 3, punto di consegna).
Una volta consegnato il messaggio, il Gestore PEC destinatario invia una ricevuta di avvenuta consegna all'utente mittente (passi 4 e 5) che può essere quindi certo che il suo messaggio è giunto a destinazione.
Nell'istante in cui invia il proprio messaggio, l'utente ha la possibilità di decidere il tipo di ricevuta tra le seguenti:

- Completa: contiene, oltre ai dati di certificazione, il messaggio originale in allegato; con questa ricevuta il mittente può verificare che il messaggio consegnato sia effettivamente quello spedito.
- Breve: contiene, oltre ai dati di certificazione, i c.d. "hash crittografici" del messaggio originale. Questo tipo di ricevuta è stata introdotta per ridurre le dimensioni dei messaggi trasmessi. Il mittente ha la possibilità di verificare che il messaggio consegnato sia effettivamente quello spedito a patto di conservare gli originali *inalterati* degli allegati al messaggio inviato.
- Sintetica: contiene i soli dati di certificazione.

Durante la trasmissione di un messaggio attraverso 2 caselle di PEC vengono emesse altre ricevute che hanno lo scopo di garantire e verificare il corretto funzionamento del sistema e di mantenere sempre la transazione in uno stato consistente.
In particolare:

- Il punto di accesso, dopo aver raccolto il messaggio originale, genera una ricevuta di accettazione che viene inviata al mittente; in questo modo chi invia una mail certificata sa che il proprio messaggio ha iniziato il suo percorso.
- Il punto di ricezione, dopo aver raccolto il messaggio di trasporto, genera una ricevuta di presa in carico che viene inviata al Gestore mittente; in questo modo il Gestore mittente viene a conoscenza che il messaggio è stato preso in custodia da un altro Gestore.

Quanto sopra riportato descrive il funzionamento di un sistema di PEC nel caso in cui non si verifichino problemi durante la spedizione.
La PEC, sfruttando crittografia e protocolli di sicurezza riesce a fornire agli utenti un servizio sicuro che sostituisce integralmente il tradizionale servizio di posta (elettronica e cartacea), mettendosi inoltre al riparo da spam, abusi e disguidi.
Questo e' possibile in quanto la posta certificata ha le seguenti caratteristiche:
- garantisce che il messaggio proviene da un gestore della PEC e da uno specifico indirizzo e-mail certificato;

- garantisce che il messaggio non può essere alterato durante la trasmissione;
- garantisce la privacy totale della comunicazione, avvenendo lo scambio dati in ambiente sicuro;
- garantisce al mittente la certezza dell'avvenuto recapito dell'e-mail alla casella di posta certificata destinataria, con la spedizione di una ricevuta di consegna, in modo analogo alla tradizionale raccomandata A/R (e con lo stesso valore legale);
- garantisce il destinatario da eventuali contestazioni in merito ad eventuali messaggi non ricevuti e dei quali il mittente sostiene l'avvenuto l'invio;
- garantisce in modo inequivocabile l'attestazione della data di consegna e di ricezione del messaggio e conserva la traccia della comunicazione avvenuta fra mittente e destinatario.

Fra le caratteristiche salienti va notato che nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte venga conservata in base al

Decreto per 30 mesi in un apposito registro informatico custodito dai gestori stessi: tale registro ha lo stesso valore giuridico delle ricevute.
Nel caso in cui le e-mail vengono inviate da caselle di PEC a caselle di posta tradizionale, vengono recapitate normalmente anche se, in questo caso, il destinatario si vedrà recapitare il messaggio originale “imbustato” all'interno di un altro messaggio.
Nel caso in cui il mail server remoto segnali l'impossibilità di consegnare il messaggio, il Gestore invia al mittente certificato un'anomalia di messaggio contenente, in allegato, il motivo della mancata consegna.
Viceversa, i messaggi provenienti da caselle tradizionali a caselle di PEC possono essere gestiti in due modi a discrezione del titolare:

- possono essere scartati
- possono essere inoltrati su un indirizzo convenzionale scelto dal Cliente.

Il Gestore non consente infatti l'ingresso verso caselle PEC di messaggi provenienti da caselle di posta elettronica convenzionale.
Il titolare del servizio, attraverso il servizio di “Inoltro”, ha però la possibilità di re-indirizzare tali messaggi verso una casella di posta elettronica convenzionale scelta dall’utente tramite accesso all'interfaccia di gestione della casella. Una volta completata l'operazione, tutti i messaggi convenzionali diretti alla casella PEC verranno indirizzati in maniera automatica verso la casella convenzionale indicata.

Contenuti del sistema di Firma Digitale (FD)
La firma digitale, o firma elettronica qualificata, basata sulla tecnologia della crittografia a chiavi asimmetriche, è un sistema di autenticazione di documenti digitali equivalente, a termini di legge, alla firma autografa su carta.
La firma digitale è un sistema di autenticazione forte in quanto si basa sull'uso di un certificato digitale memorizzato su di un dispositivo hardware che consente di attestare per un documento sottoscritto:

- l’autenticità: certezza dell'identità del sottoscrittore;
- la paternità: l’impossibilità che il firmatario disconosca il documento sottoscritto;
- l’integrità: la certezza che il documento non sia stato modificato dopo essere stato firmato digitalmente.
- Non ripudio: riconducibilità al titolare del dispositivo di firma, salvo che venga data prova contraria.
- Valore legale: il documento informatico sottoscritto con firma elettronica qualificata o con FD soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 del D.Lgs 7 marzo 2005, n. 82-CAD che garantiscano l'identificabilità dell'autore e l'integrità del documento.

L'elemento di rilievo del sistema di autenticazione è rappresentato dal certificato digitale di autenticazione che il Gestore rilascia al titolare di una smart card.
Il certificato di autenticazione è un file che permette di firmare la propria posta elettronica o di autenticarsi ai siti web, in modalità sicura.
Quando il certificato di autenticazione viene usato per accedere ad un indirizzo web, non solo il browser si accerta dell'identità del server ma consente anche al server di accertare l'identità della persona che utilizza il browser.
In base a tale conoscenza il server consentirà l'accesso ad aree di informazioni riservate piuttosto che ad altre.
Quando il certificato di autenticazione viene usato per firmare un messaggio di posta elettronica, esso risulta associato al messaggio stesso, arricchendolo di informazioni anagrafiche sul mittente, quali cognome e nome, che permettono di stabilirne con certezza la provenienza.
Il certificato di autenticazione, infatti, abbina, da una parte, i dati del mittente ad un indirizzo di posta elettronica; dall'altra riporta i dati dell'Ente Certificatore che lo ha rilasciato.
Il servizio FD utilizza i protocolli di posta S/MIME e quelli di accesso sicuro SSL.

Il servizio di marcatura temporale di un documento informatico, consiste nella generazione, da parte di una *Terza Parte Fidata*, di una firma digitale del documento (anche aggiuntiva rispetto a quella del sottoscrittore) cui è associata l'informazione relativa ad una data e ad un'ora certa.
L'art. 16, c.6 del D.L. n. 185/2008, obbliga i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato a comunicare ai rispettivi ordini o collegi il proprio indirizzo di PEC entro il 29 novembre 2009.