CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

La posta elettronica certificata

11

Redazione a cura di
Claudio Petrucci
Marco Orazi
Francesco Tortorelli

Con la collaborazione di
Progetto Europa Consulting

Supplemento al n. 1/2007 del periodico Innovazione,
registrato al Tribunale di Roma n. 523/2003
Direttore Responsabile Franco Tallarita

CNIPA – Centro nazionale per l'informatica nella pubblica amministrazione
Via Isonzo, 21/b - 00198 Roma
Tel. 06.85264.1 - www.cnipa.gov.it

Stampa Stilgrafica Srl
Via I. Pettinengo, 31/33 - 00159 Roma
Tel. 0643588200 - Fax 064385693

La posta elettronica certificata

A cura di
Claudio Petrucci, Marco Orazi
Francesco Tortorelli

con la collaborazione di
Progetto Europa Consulting srl

CNIPA
Via Isonzo, 21/b - 00198 Roma
Tel.: 06 85264.1
www.cnipa.gov.it

Sommario

La posta elettronica certificata

Introduzione

La posta elettronica rappresenta uno strumento di ampissima diffusione per le caratteristiche di semplicità, immediatezza ed efficacia ed è frequentemente utilizzata nelle comunicazioni interpersonali e d'ufficio, per scambi di messaggi, nella gestione di appuntamenti, trasmissione di file e documenti digitali di qualsiasi genere. Le informazioni scambiate, talvolta anche a carattere formale, riguardano prevalentemente utenti tra loro noti. D'altra parte la diffidenza ad utilizzare la posta elettronica, tra soggetti generalmente tra loro non noti o quando la comunicazione assume un valore legale, è giustificata da alcune "debolezze" intrinseche dello strumento. Utenti con un pochino di esperienza con la posta elettronica possono facilmente falsificare il mittente, l'orario di invio, la notifica di ricezione e quant'altro. Inoltre, alla posta elettronica tradizionale mancano la standardizzazione delle ricevute e dei comportamenti dei provider, sia nei casi di attribuzione delle caselle sia nel trattamento delle mail in caso di anomalia. Infine, è opportuno aggiungere che chiunque, dotato anche di un solo personal computer, può realizzare un sistema completo di posta elettronica, gestendo in autonomia il servizio. È evidente pertanto che la posta elettronica, pur essendo uno strumento facilmente accessibile da qualsiasi utilizzatore, non fornisce né garanzie certe di effettivo invio e consegna di un messaggio, né certezza sulla sua paternità, né regole standardizzate che consentano di tracciare il percorso del messaggio durante la fase di trasmissione.

La posta elettronica certificata (PEC) è un sistema di posta elettronica in grado di superare le "debolezze" della posta elettronica e di poter essere utilizzata in qualsiasi contesto nel quale sia necessario avere prova opponibile dell'invio e della consegna di un documento elettronico. La posta elettronica certificata si presenta come un'innovazione capace di generare enormi risparmi sul piano economico nei settori pubblici e privati e di semplificare i rapporti tra privati e tra costoro e la Pubblica Amministrazione.

La normativa, necessaria in un paese come l'Italia dove il diritto trae fondamento da una tradizione scritta (civil law), ha stabilito il formato delle ricevute e le caratteristiche tecniche di funzionamento, ha inoltre introdotto e disciplinato, nell'ordinamento italiano, la figura del Gestore del servizio di posta elettronica certificata (fornitore del servizio).
Utilizzando un parallelo con il mondo cartaceo, potremmo dire che la posta elettronica sta alla lettera ordinaria come la posta elettronica certificata sta alla raccomandata; considerazione aggiuntiva è che il sistema di posta elettronica certificata risolve alcune carenze intrinseche della raccomandata tradizionale:

- la conoscibilità certa della casella mittente e quindi del titolare, mentre non è tracciato colui che spedisce una raccomandata;
- la possibilità di legare in maniera certa ed opponibile la trasmissione con il documento trasmesso, tale possibilità è preclusa con la raccomandata.

Un'ulteriore caratteristica della posta elettronica certificata è quella di essere adatta tanto ad uno scambio tra individui quanto a quello tra applicazioni. Un'organizzazione può ricevere attraverso messaggi di posta elettronica certificata documenti che possono essere immediatamente trattati da un'applicazione informatica, grazie alle caratteristiche delle ricevute.
L'utente abituato all'utilizzo della posta elettronica non dovrà cambiare abitudini operative o installare particolari software e potenzialmente potrà inviare o ricevere raccomandate elettroniche in una qualunque ora e giorno dell'anno da un qualunque dispositivo collegato ad una rete telematica. L'utente che voglia utilizzare la posta elettronica certificata potrà contare su livelli minimi di servizio garantiti dalla norma ed una trasparenza delle offerte garantita dalla pubblicazione in internet, da parte di ogni gestore, di un manuale operativo relativo al servizio offerto. In tale manuale, tra l'altro, l'utente può trovare le caratteristiche di ciascuna offerta e può in questo modo orientarsi tra le diverse proposte che, oltre al rispetto dei numerosissimi requisiti tecnici, contengono servizi aggiuntivi che valorizzano e differenziano le singole proposte.
Il lettore può trovare in questa minigrafia la descrizione della posta elettronica certificata, le modalità di funzionamento, le funzionalità base a disposizione degli utenti, alcuni suggerimenti per l'utilizzo, gli ambiti di applicazione del servizio e le caratteristiche dei gestori.

Il quadro normativo di riferimento

A partire dal riferimento primario costituto dall'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 il quadro normativo relativo alla Posta Elettronica Certificata è costituito dai seguenti riferimenti:

- Decreto del Presidente della Repubblica
- Decreto Ministeriale
- Circolare di accreditamento CNIPA
- Circolare di vigilanza CNIPA
- Decreto Legislativo (Codice dell'Amministrazione Digitale)

- DPR 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. 28 aprile 2005, n. 97)
- Decreto Ministeriale 2 novembre 2005, "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (G.U. del 14 novembre 2005, n. 265)
- Circolare di accreditamento CNIPA CR/49 24 novembre 2005, "Modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005 n. 68" (G.U. 5 dicembre 2005, n. 283)
- Circolare di vigilanza CNIPA CR/51 del 7 dicembre 2006, "Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68" (G.U. 21 dicembre 2006, n.296)
- Decreto Legislativo 7 marzo 2005, n. 82 (G.U. 16 maggio 2005, n. 93)

Di seguito sono proposti gli elementi più significativi di ciascuna delle precedenti norme.

Contenuti del DPR

- definizione dei soggetti previsti dal servizio [art. 2]:
  - Mittente;
  - Destinatario;
  - Gestore;
- modifica del comma 1 dell'art. 14 del dpr 445 del 2000 [art. 3] resa necessaria per ridefinire la formulazione originaria relativa alla sequenza di invio e ricezione di un documento informatico. Di seguito è proposta la nuova formulazione, attualmente in vigore:
  - 1. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.
- obbligo per i gestori di garantire l'interoperabilità dei servizi offerti [art. 5, comma 2];
- garanzie circa l'integrità del messaggio trasmesso [art. 11, comma 1]
- obbligo per i gestori di tenere traccia delle operazioni svolte, in un apposito log, per una durata di trenta mesi garantendone la riservatezza, la sicurezza, l'integrità e l'inalterabilità [art. 11, commi 2 e 3];
- regole per la gestione dei messaggi contenenti virus [art. 12];
- obbligo per i gestori di garantire livelli minimi di servizio [art. 13];
- definizione dell'elenco pubblico dei gestori di posta elettronica certificata [art. 14, comma 1];
- elenco dei requisiti che il candidato gestore deve dimostrare di possedere per essere iscritto nell'elenco pubblico [art 14, commi 2, 3, 4, 5 e 6];
- assegnazione al CNIPA delle funzioni di vigilanza e controllo sulle attività dei gestori [art. 14, comma 13];
- limiti di utilizzo delle caselle di posta elettronica certificata rilasciate dalle PA ai privati [art. 16, comma 2].

Contenuti del DM

Il Decreto Ministeriale approfondisce parte dei contenuti proposti dal DPR e prevede come allegato l'insieme dei requisiti tecnico/funzionali necessari alla realizzazione di una piattaforma software per l'erogazione del servizio. In particolare, introduce nuovi elementi di dettaglio relativi a:

- obbligo per il gestore di acquisire la certificazione ISO 9001:2000 relativamente a tutti i processi connessi al servizio di posta elettronica certificata [art. 20];
- definizione dei requisiti organizzativi dei gestori [art. 21/22/23].

Contenuti della circolare di accreditamento

La circolare di accreditamento fornisce elementi di dettaglio per la presentazione della domanda di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata. In particolare, la documentazione richiesta è relativa ai seguenti ambiti:

- societario;
- economico-patrimoniale;
- organizzativo;
- tecnico-operativo/sicurezza.

La circolare fornisce inoltre indicazioni circa la modalità di esame della domanda di iscrizione all'elenco pubblico dei gestori.

Contenuti della circolare di vigilanza

La circolare di vigilanza fornisce elementi di dettaglio in relazione alle modalità con le quali il CNIPA esercita la vigilanza nei confronti dei gestori iscritti nell'elenco pubblico e prevede:

- lo svolgimento dei test di interoperabilità;
- il monitoraggio, da parte del CNIPA, delle modalità di vendita dei servizi PEC;
- la comunicazione periodica al CNIPA delle statistiche relative al traffico gestito ed ai livelli di servizio erogati;
- la tempestiva segnalazione al CNIPA di malfunzionamenti gravi al proprio servizio di posta elettronica certificata;

- la sospensione del servizio erogato dal gestore in caso di malfunzionamenti gravi;
- l'effettuazione di sopralluoghi da parte del CNIPA presso le strutture utilizzate dal gestore, al fine di verificare la conformità del sistema di PEC;
- la disposizione, da parte del CNIPA, di provvedimenti nei confronti dei gestori inadempienti.

Contenuti del Codice dell'Amministrazione Digitale

Il Codice dell'Amministrazione Digitale rappresenta uno strumento giuridico volto a fornire un quadro normativo coerente, omogeneo ed unitario all'applicazione delle nuove tecnologie nella PA.
Il Codice, relativamente alla posta elettronica certificata, prevede:

- il diritto all'uso delle tecnologie [art. 3];
- indicazioni circa l'utilizzo della posta elettronica certificata per la PA [art.6];
- obbligo di istituire almeno una casella di posta elettronica certificata, per ciascun registro di protocollo [art. 47];
- l'utilizzo della posta elettronica certificata nei casi per i quali è necessaria l'evidenza dell'avvenuto invio e ricezione di un documento informatico [art.48]

Tutta la normativa sopra descritta è interamente presente e scaricabile dall'apposita sezione del sito del Cnipa.

Per completezza, e per chiudere con gli interventi normativi predisposti dal legislatore, la legge Finanziaria 2008 richiama la posta elettronica certificata, all'articolo 2 comma 589, prevedendo che il CNIPA effettui azioni di monitoraggio e verifica, presso le pubbliche amministrazioni, delle disposizioni in materia di posta elettronica certificata. Il mancato adeguamento alle predette disposizioni in misura superiore al 50 per cento del totale della corrispondenza inviata comporta la riduzione, nell'esercizio finanziario successivo, del 30 per cento delle risorse stanziate nell'anno in corso per spese di invio della corrispondenza cartacea.

Come funziona la PEC

In questo capitolo viene proposta la descrizione funzionale del servizio con l'evidenza di tutti gli "attori", a vario titolo coinvolti nel processo di invio/ricezione di un documento informatico.
Iniziamo, quindi, elencando quali sono le componenti da considerare:

- l'utente mittente, cioè colui il quale 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.

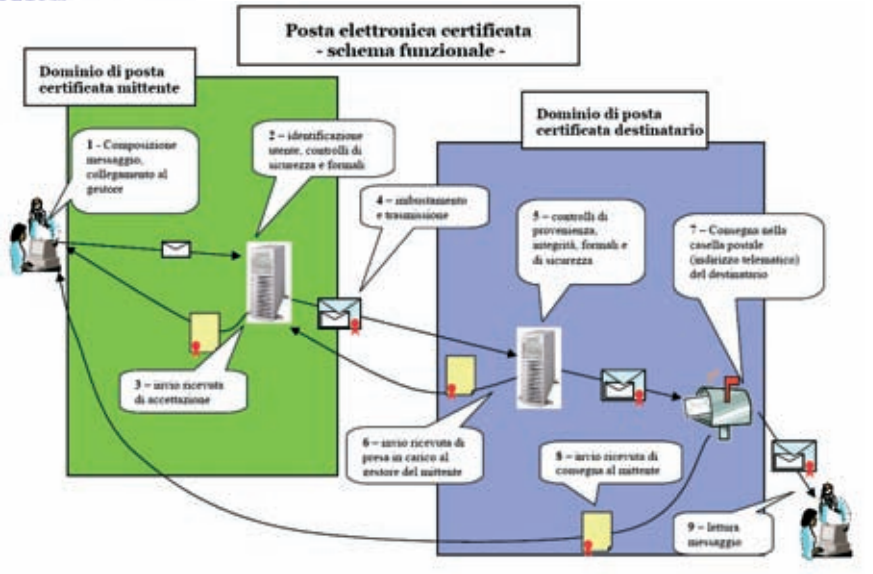
Predisposto l'oggetto dell'invio, il mittente, si deve far riconoscere dal sistema di PEC del proprio gestore secondo le modalità da questi previste. Una modalità diffusa per accedere al servizio PEC è ad esempio la classica accoppiata user-id/password; ciò non toglie la possibilità di adottare modalità 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 finalizzati 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, destinate 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. Il verificarsi di 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 la presenza nella ricevuta dell'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.
Ora il destinatario ha disponibile nella sua casella il messaggio ricevuto, e può quindi consultarlo, come in un sistema di posta elettronica tradizionale. È importante evidenziare che il sistema di PEC, essendo un sistema di trasporto, non considera la lettura del messaggio prova dell'effettiva consegna. Il messaggio si intende consegnato quando il Gestore lo rende disponibile nella casella di posta elettronica certificata del destinatario.
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.
Di seguito è proposta una rappresentazione grafica di quanto appena esposto.



Una descrizione più tecnica ed approfondita delle operazioni che vengono svolte all'interno della posta elettronica certificata e finalizzate ad aumentarne la tracciabilità, l'affidabilità e la sicurezza del sistema, è contenuta nella normativa tecnica di riferimento (Regole tecniche allegate al DM). Un commento relativo a tali funzionalità e caratteristiche esula dagli scopi del presente minigrafia.

Il punto di vista dell'utente

La posta elettronica certificata è ormai una realtà che cambierà molte modalità di comunicazione non solo fra le imprese, ma anche fra queste e la Pubblica Amministrazione; inoltre, anche i normali cittadini avranno un notevole risparmio di tempo e denaro comunicando con la Pubblica Amministrazione utilizzando questo nuovo sistema, quando fino a ieri era possibile utilizzare solo la tradizionale raccomandata A/R. Qualunque cittadino o impresa oggi può rivolgersi ad uno dei fornitori del servizio (Gestori) iscritti nell'apposito elenco pubblico gestito dal CNIPA (vedi la sezione "I Gestori") ed ottenere, previa sottoscrizione di un contratto, una casella di PEC. I Gestori di posta elettronica certificata possono essere sia aziende che Pubbliche Amministrazioni ma in en-

trambi i casi devono aver superato con successo l'istruttoria di accreditamento del CNIPA, che ha come scopo la verifica del possesso dei requisiti organizzativi e tecnici, nonché di sicurezza – stabiliti dalla norma – per l'erogazione del servizio, al fine di garantire una qualità dei servizi offerti all'utenza coerente con il dettato e lo spirito della norma.
La scelta del Gestore da utilizzare come fornitore del servizio di PEC dovrebbe essere fatta sia in base alle proprie esigenze che alle offerte tecniche e commerciali che ciascun Gestore propone, disponibili sul sito Internet dichiarato nella fase di accreditamento presso il CNIPA. Inoltre, ciascun Gestore è obbligato per legge a pubblicare sul proprio sito anche il Manuale Operativo del servizio, che descrive, tra l'altro, le soluzioni tecniche adottate per l'accesso e l'utilizzo della propria casella e per garantire i previsti livelli di sicurezza nella trasmissione.
L'offerta di ciascun Gestore di Posta Elettronica Certificata, benché debba rispettare i livelli minimi di servizio e i requisiti imposti dalla norma, può variare nel dettaglio: l'utente può stipulare un contratto con il proprio Gestore richiedendo singole caselle, un intero dominio cui fanno capo più caselle, oltre che ulteriori servizi non regolamentati. Dopo aver stipulato un contratto con il fornitore prescelto, l'attivazione della(e) casella(e) di PEC avviene seguendo la procedura definita dal fornitore e descritta nel Manuale Operativo predetto. Dopo l'attivazione della casella di PEC ogni utente ha a disposizione tutti i servizi, normati e non, che il Gestore mette a disposizione: gestione completa della casella (lettura, cancellazione, spostamento, etc. dei messaggi), gestione delle ricevute di invio e ricezione opponibili a terzi in caso di contestazione, accesso ai log delle operazioni svolte in caso di smarrimento delle ricevute; tutto questo rispettando i livelli minimi di qualità del servizio stabiliti dalla Norma.
L'utilizzo della PEC è assimilabile a quello della posta elettronica tradizionale, se si esclude la produzione delle ricevute e la gestione dei dati di certificazione (firma dei messaggi e delle ricevute/avvisi). Per la fruizione del servizio si può impiegare sia un normale browser di pagine Internet come, a solo titolo di esempio, Internet Explorer che uno dei client di posta tra quelli diffusi sul mercato. La norma, tuttavia, impone che i client rispettino almeno i seguenti requisiti:

- gestione del colloquio con i punti di accesso e di consegna utilizzando canali di trasmissione sicuri;

- gestione dell'autenticazione dell'utente sia in fase di invio che di ricezione dei messaggi;
- gestione della firma elettronica apposta sui messaggi e sulle ricevute, nonché sugli eventuali avvisi.

Per un elenco completo e maggiormente dettagliato delle caratteristiche dei client per l'utilizzo della PEC si rimanda alle Regole Tecniche allegate al Decreto Ministeriale 2 novembre 2005.
Mediante il servizio di posta elettronica certificata è possibile spedire qualunque tipo di documento prodotto con strumenti informatici (anche sottoscritto con firma digitale); tuttavia, proprio per le sue caratteristiche peculiari, è preferibile utilizzarlo nelle comunicazioni "ufficiali" che richiedono la certificazione delle fasi di invio e ricezione del messaggio e degli eventuali allegati, come ad esempio l'invio di documentazione ad una Pubblica Amministrazione. Benché sia preferibile utilizzare il servizio di PEC per questo tipo di comunicazioni, ciò non esclude il suo impiego anche per i casi in cui non sia necessario disporre delle certificazioni prodotte.
L'utente mittente del servizio di posta elettronica certificata (identificato dal Gestore come il titolare della casella) riceve nella propria casella, se il processo di invio e ricezione va a buon fine, due ricevute: una di accettazione da parte del proprio Gestore e una di avvenuta consegna da parte del Gestore del destinatario. Qualora una ricevuta venga inavvertitamente cancellata oppure smarrita, il titolare può richiedere al proprio Gestore, utilizzando i canali e le modalità che quest'ultimo mette a disposizione alcune informazioni in essa contenute. Questa possibilità, garantita dalla norma, è volta alla salvaguardia del titolare in caso di contenzioso nel quale si richieda documentazione attestante l'invio e la ricezione di un messaggio; tuttavia, è bene sottolineare che l'archivio delle operazioni svolte (log), dal quale è possibile risalire alle informazioni contenute nelle le ricevute, deve essere conservato dal Gestore per trenta mesi.
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. Inoltre, il destinatario di un messaggio di PEC non può negarne l'avvenuta ricezione, dal momento che

la ricevuta di avvenuta consegna, firmata ed inviata al mittente dal Gestore di PEC scelto dal destinatario, riporta la data e l'ora in cui il messaggio è stato consegnato nella casella di PEC del destinatario, certificandone, di fatto, l'avvenuta consegna. Come ulteriore valore aggiunto rispetto alla raccomandata cartacea, la PEC consente non solo di certificare le fasi di invio e ricezione di un messaggio ma, utilizzando la ricevuta di avvenuta consegna "completa" (che riporta anche tutti gli eventuali allegati), si può certificare che il contenuto ricevuto è esattamente quello che era stato inviato.
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 Decreto Ministeriale 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.

Il punto di vista del Gestore

I Gestori del servizio di posta elettronica certificata, iscritti nell'apposito elenco pubblico gestito dal CNIPA, svolgono il ruolo di garante per le fasi di invio e di consegna di un messaggio, oltre ovviamente a rilasciare caselle e domini PEC. Secondo quanto previsto dalla Norma, possono svolgere il ruolo di Gestori sia aziende private, con capitale sociale non inferiore ad un milione di euro, sia Pubbliche Amministrazioni, purché presentino regolare domanda di accreditamento presso il CNIPA

che, a seguito di una istruttoria, valuta se il richiedente possiede i requisiti minimi previsti dalla norma per lo svolgimento dell'attività di Gestore. L'elenco pubblico dei Gestori di Posta Elettronica Certificata è disponibile per la consultazione sul sito del CNIPA, come mostrato nella figura seguente.

Il CNIPA, nel corso dell'istruttoria di accreditamento, valuta, tra gli altri, i requisiti di onorabilità, l'adeguatezza del personale, i processi atti a garantire la sicurezza dei dati e delle trasmissioni, l'esperienza del proponente nell'erogazione di servizi di analoga natura, la ridondanza ed i servizi messi in atto in caso di emergenza. È bene sottolineare che tutti i Gestori iscritti nell'elenco pubblico possiedono i requisiti minimi previsti dalla norma, per cui sono equiparabili sia dal punto di vista tecnico che organizzativo, tuttavia l'offerta commerciale del servizio può differire; prima di scegliere un Gestore di PEC, quindi, è bene valutare le diverse offerte proposte visitando il sito Internet dichiarato dal Gestore e presente nell'elenco pubblico.

Tutti i Gestori, in fase di accreditamento, assumono alcuni obblighi, sia nei confronti degli utenti che del CNIPA, tra i quali:

- rispettare i requisiti previsti dalla norma per lo svolgimento dell'attività di Gestore;
- rispettare le prescrizioni previste dalle Regole Tecniche allegate al Decreto Ministeriale 2 novembre 2005;
- dotarsi di una certificazione ISO specifica per il processo di erogazione del servizio PEC;
- dotarsi di una polizza assicurativa a copertura dei danni derivanti dall'attività di Gestore;
- fornire tutti gli aggiornamenti in merito alla struttura organizzativa, all'assetto societario, alle caratteristiche del servizio, all'organizzazione della sicurezza e alle sedi presso le quali il servizio viene erogato;
- consentire l'accesso, da parte di incaricati del CNIPA, alle sedi dedicate all'erogazione del servizio, affinché gli stessi possano espletare l'attività di vigilanza.

Come detto in precedenza, non solo le aziende private ma anche le Pubbliche Amministrazioni possono svolgere il ruolo di Gestori di Posta Elettronica Certificata. Tuttavia, come stabilito dall'art. 16 del DPR, le caselle rilasciate ai privati da una Pubblica Amministrazione possono essere utilizzate esclusivamente per comunicazioni tra la stessa e l'utente cui è stata rilasciata la casella. Lo stesso DPR, all'art. 15, stabilisce che il servizio di PEC sul territorio italiano può essere erogato anche da Gestori stabiliti in altri paesi dell'Unione europea che soddisfino, in accordo alla legislazione dello stato membro di riferimento, formalità e requisiti equivalenti al DPR e al DM; il CNIPA valuta l'equivalenza dei requisiti.

La PEC dal punto di vista della PA

L'utilizzo della posta elettronica certificata rappresenta per la Pubblica Amministrazione un'opportunità ed un obbligo al tempo stesso. È un'opportunità in quanto consente di ammodernare i propri processi di comunicazione aumentando l'efficienza e riducendo i costi. Studi di

fattibilità relativi a diversi progetti di utilizzo della posta elettronica certificata hanno dimostrato l'enorme recupero di efficienza e i risparmi diretti e indiretti. Come già ricordato la PEC è uno strumento di trasporto e pertanto la sua adozione in luogo di strumenti tradizionali può rendere efficiente solo questa parte del processo. Come si accennava, il codice dell'amministrazione digitale (L. 82/05) stabilisce che i privati hanno diritto a richiedere e ottenere l'uso della PEC da parte delle amministrazioni, le quali ai sensi della l. 82/05, art. 47, devono istituire almeno una casella di posta elettronica certificata.
La suddetta norma stabilisce inoltre che gli indirizzi delle caselle di posta elettronica certificata delle amministrazioni devono essere resi disponibili anche attraverso il sito web dell'amministrazione stessa.
Le pubbliche amministrazioni garantiscono ai terzi la libera scelta del Gestore di posta elettronica certificata da utilizzare nelle comunicazioni con le stesse[art. 16 DPR], mentre l'utilizzo nei confronti dei privati della posta elettronica certificata deve essere da questi esplicitamente richiesto fornendo il proprio indirizzo. La dichiarazione di tale indirizzo è giuridicamente valida nell'ambito di ciascun procedimento. A tal fine è opportuno che le amministrazioni, che intendono utilizzare la PEC nei confronti dei privati che accettano tale canale di comunicazione, richiedano espressamente il consenso per tutti i procedimenti per i quali sono in grado di comunicare attraverso la PEC stessa. In tal modo può essere ottimizzato il processo di acquisizione della volontà dei privati nei casi in cui costoro preferiscano questo canale di comunicazione. Le amministrazioni dovranno inoltre considerare che la volontà possa essere revocata ovvero il privato può comunicare una variazione di indirizzo di posta elettronica certificata. Occorre tener presente che allo stato attuale della normativa l'indirizzo di posta elettronica certificata non può essere considerato come una residenza telematica e non esistono elenchi pubblici di indirizzi di posta elettronica certificata di privati. A tale affermazione fa parziale eccezione la pubblicazione (su base volontaria) degli indirizzi di posta elettronica certificata delle imprese, all'atto di iscrizione nel registro delle imprese. Tale volontà manifesta l'assenso ad accettare l'utilizzo della posta elettronica certificata limitatamente ai rapporti tra privati [art. 4 DPR].
La norma, come accennato in precedenza, prevede che la Pubblica Amministrazione possa essere anche gestore di posta elettronica certificata. In questo caso la PA può operare:

- limitatamente ai propri bisogni di caselle di posta elettronica certificata;
- fornendo le caselle PEC anche ad altre amministrazioni;
- fornendo le caselle anche ai privati.

In linea generale mentre gli adempimenti amministrativi e i vincoli previsti dalla normativa risultano semplificati per la Pubblica Amministrazione, le caratteristiche ed i vincoli tecnici sono perfino superiori a quelli previsti per i privati. Pertanto la PA come gestore di posta elettronica certificata deve considerarsi un fatto eccezionale o giustificato da una reale specificità.
In tutti i casi suddetti, la PA deve dimostrare di avere tutti i requisiti tecnici e organizzativi, con particolare riguardo a metodi e procedure per la gestione del servizio. Nella predetta circostanza la Pubblica Amministrazione oltre alle responsabilità derivanti dall'azione amministrativa aggiunge quelle tipiche dell'esercizio del servizio di posta elettronica certificata.
L'esercizio dell'attività di gestore da parte di una PA deve limitarsi alla sussidiarietà, senza imposizione, in quanto il privato, come già ricordato, può utilizzare un qualunque Gestore. Sul piano tecnico la PA deve impedire che le caselle fornite ai privati possano essere da questi utilizzate per comunicare con altri soggetti, pubblici e privati.
In ultima analisi si ritiene che le necessità che possono suggerire ad una PA di scegliere di diventare gestore possano essere soddisfatte utilizzando altri Gestori (privati), studiando una soluzione specifica. Il CNIPA può fornire il necessario supporto per valutare attentamente una tale scelta.

Il ruolo del CNIPA e le iniziative di sostegno

Il servizio di posta elettronica certificata nasce all'interno del CNIPA che ha avviato negli scorsi anni una lunga fase di confronto e sperimentazione, informando attraverso il proprio sito delle attività in corso e delle caratteristiche del servizio, man mano che si andava consolidando sul piano tecnico e normativo. Tale fase di sperimentazione ha coinvolto diverse categorie di soggetti consentendo in tal modo di far crescere un mercato nel quale la Pubblica Amministrazione si è trovata al centro di un processo di innovazione. La posta elettronica certificata ha già

una consistente distribuzione, alla data di scrittura del presente si contano 23 gestori iscritti nell'apposito elenco, circa 16.000 sono il numero di domini PEC complessivamente gestiti dai 23 soggetti, per un rilevante numero di caselle distribuite.
I fornitori di tecnologie di posta elettronica hanno da tempo provvisto di "moduli di posta certificata" i loro sistemi, siano essi proprietari che open source. L'approccio utilizzato e la contestuale promozione svolta dal CNIPA, attraverso diverse azioni sussidiarie ed il cofinanziamento di progetti, hanno contribuito allo sviluppo della posta elettronica certificata nella Pubblica Amministrazione. Tra le applicazioni significative della PEC in ambito Pubblica Amministrazione segnaliamo:

- l'iniziativa dell'Agenzia delle Entrate che con Provvedimento del Direttore del 22 dicembre 2005, prevede che ciascun operatore finanziario è tenuto a dotarsi di un indirizzo di posta elettronica certificata (PEC), tramite il quale riceve le richieste di indagine da parte degli organi a ciò preposti;
- la sperimentazione del Ministero di grazia e giustizia nell'ambito del Processo telematico civile. Il progetto consiste nella realizzazione di un insieme di applicazioni informatiche e infrastrutture tecnologiche che renda accessibile via web il sistema informatico civile, sia per il deposito di atti che per attività di consultazione dello stato delle cause e del fascicolo elettronico; inoltre è prevista anche la trasmissione per via telematica di comunicazioni, notifiche e copie di atti dagli uffici giudiziari ai soggetti coinvolti;
- la richiesta della Magistratura che tutte le comunicazioni relative alle intercettazioni telefoniche avvengano tramite posta elettronica certificata.

La normativa sulla posta elettronica certificata attribuisce al CNIPA diverse responsabilità. Innanzitutto il CNIPA è custode e gestore delle regole tecniche e provvede al loro aggiornamento in funzione dell'evoluzione tecnologica e dell'esperienza derivante dall'utilizzo del sistema. In tali circostanze il CNIPA provvede alla necessaria pubblicizzazione degli aggiornamenti, in coerenza con gli standard specificati nella normativa [art. 4 DM]. In questo caso, per le regole tecniche, il sito del CNIPA funge da "riferimento ufficiale". Il CNIPA gestisce l'elenco pubblico dei gestori di posta elettronica certificata [art. 14 DPR]. In tale ambito accoglie

e valuta le domande presentate dai soggetti che si candidano al ruolo di gestori di posta elettronica certificata, decretandone l'iscrizione nell'apposito elenco o respingendone la domanda, per carenze di requisiti. Ai soggetti iscritti il CNIPA fornisce i certificati per la firma elettronica delle ricevute [art. 7 DM] e per l'accesso e l'aggiornamento della struttura tecnica che costituisce l'insieme dei domini di posta elettronica certificata [art. 18 DM], definita indice dei gestori PEC (IGPEC). Al CNIPA vanno presentate tutte le modifiche in ordine all'assetto societario, alle caratteristiche del servizio, alle procedure adottate, con particolare riguardo agli aspetti di continuità di funzionamento e di sicurezza, in tal caso il CNIPA si riserva di riaprire una parziale istruttoria.

Il CNIPA svolge inoltre il ruolo di vigilanza e controllo sulle attività esercitata dai gestori iscritti nell'elenco [art. 14 DPR]. A tal riguardo emette circolari esplicative e di indirizzo, acquisisce informazioni, esegue test di interoperabilità del sistema di gestione della PEC [ai sensi dell'art.5 DPR] e può accedere presso le sedi dei gestori per effettuare attività di verifica circa la conformità del sistema PEC. Nello svolgimento delle proprie attività il CNIPA si relaziona agli altri organismi quali: autorità per la concorrenza e il mercato, autorità garante per la privacy, autorità giudiziaria, altre istituzioni interessate per materia.

Il CNIPA gestisce il sito www.IndicePA.gov.it che contiene la struttura organizzativa delle amministrazioni, gli Uffici di protocollo (AOO – Aree Organizzative Omogenee), le caselle di posta elettronica ufficiali e le caselle di posta elettronica certificata.

Le amministrazioni possono nell'ambito del Sistema Pubblico di Connettività e Cooperazione, richiedere (facoltativamente) il servizio di posta elettronica certificata, così come previsto nel lotto 2 alla voce servizi di interoperabilità evoluta. Il raggruppamento che si è aggiudicato la gara è composto dalle società EDS Italia ed Almaviva.

Il CNIPA, per la competenza in materia di posta certificata, fornisce supporto e diffonde la conoscenza presso le amministrazioni ed i privati attraverso iniziative strutturate e interloquendo con coloro che hanno necessità di approfondimenti sul tema e specifici quesiti.

La legge finanziaria 2008, come in precedenza richiamato, dispone che il CNIPA effettui azioni di monitoraggio e verifica, presso le Pubbliche Amministrazioni, delle disposizioni in materia di posta elettronica certificata.

I gestori

Ad oggi risultano accreditati i seguenti Gestori:

- **Actalis S.p.A.**
- **Amministrazione Provinciale di Nuoro**
- **Ancitel S.p.A.**
- **Aruba PEC S.p.A.**
- **Cedacri S.p.A.**
- **Consiglio Nazionale del Notariato**
- **EDS Italia S.p.A.**
- **Fastweb S.p.A.**
- **I.NET S.p.A.**
- **Infocert S.p.A.**
- **IN.TE.S.A. S.p.A.**
- **ITnet S.r.l.**
- **IT Telecom S.r.l.**
- **IWBank S.p.A.**
- **Lombardia Integrata S.p.A.**
- **Namirial S.p.A.**
- **Numera Sistemi e Informatica S.p.A.**
- **Postecom S.p.A.**
- **Poste Italiane S.p.A.**
- **Regione Marche**
- **Sogei – Società Generale d'Informatica S.p.A.**
- **Tecnopolis Csata S.c.a.r.l.**
- **TWT S.p.A.**

È da segnalare che non tutti i Gestori accreditati hanno avviato l'operatività del servizio.
La versione aggiornata dell'elenco dei Gestori, firmato digitalmente dal Presidente del CNIPA, è disponibile presso il sito del CNIPA all'indirizzo: http://www.cnipa.gov.it.

L'utilizzo della PEC ed il mercato di riferimento

I possibili impieghi della PEC vanno oltre la sostituzione o integrazione della tradizionale raccomandata con uno strumento certamente più efficiente e anche meno costoso: d'altro canto, come sempre accade quando si parla di innovazioni tecnologiche, sarà il mercato stesso a scoprire progressivamente forme d'uso che oggi non è facile prevedere in modo completo.
Alla data di scrittura della presente minigrafia i gestori appartengono a categorie di attività eterogenee. Sono stati accreditati provider, aziende di telecomunicazioni, banche, società di servizi e Pubbliche Amministrazioni. Ognuno di questi soggetti è legato da un rapporto contrattuale con i titolari delle caselle PEC che il gestore rende disponibili.

Il CNIPA, come previsto dalla circolare di vigilanza, raccoglie periodicamente i dati relativi al servizio PEC erogato dai gestori iscritti nell'elenco pubblico. Il fine è quello di analizzarli per monitorare l'utilizzo e la diffusione della posta certificata, nonché il corretto funzionamento dei sistemi dei gestori. I risultati, disponibili sul sito del CNIPA, mostrano che l'andamento delle caselle e dei messaggi, così come per i domini, è in continua crescita. Il trend positivo dimostra come il mercato abbia compreso i vantaggi derivanti dall'applicazione della PEC e delle procedure automatizzate di gestione dei messaggi. L'analisi effettuata sui dati che misurano i livelli di servizio conferma l'affidabilità dei soggetti preposti all'erogazione del servizio.

I punti di forza della PEC

La PEC per come è stata progettata è in grado di garantire una serie considerevole di funzionalità che costituiscono dei significativi vantaggi rispetto ai servizi tradizionali oggi utilizzati. In particolare, per capire le potenzialità e le aree di applicazione della PEC, è opportuno partire da un elenco dei suoi principali punti di forza:

- certificazione dell'avvenuta consegna del messaggio nella casella di posta del destinatario del messaggio e dei suoi contenuti;
- certificazione degli allegati al messaggio;
- possibilità di allegare al messaggio qualsiasi tipologia di informazione e/o documento in formato digitale (come per l'e-mail tradizionale);

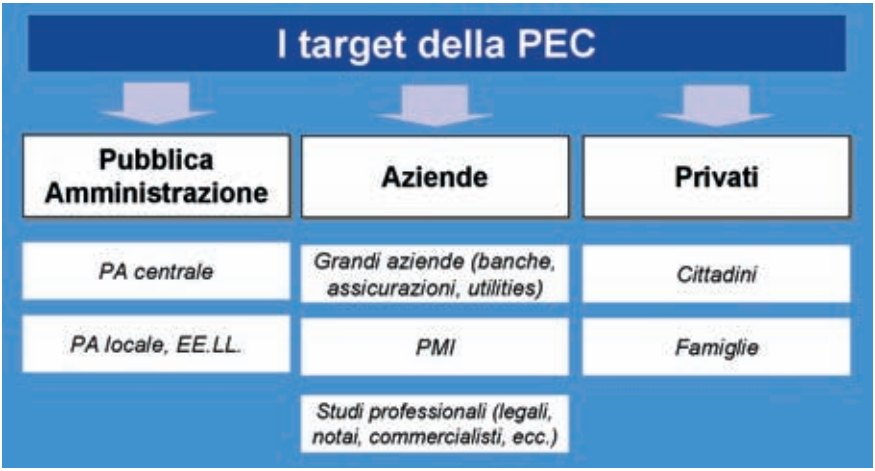
- archiviazione da parte del gestore di tutti gli eventi associati ad invii e ricezioni, per un periodo di trenta mesi;
- semplicità di trasmissione, inoltro, riproduzione, archiviazione e ricerca dei messaggi (punti di forza tipici anche dell'e-mail tradizionale);
- economicità di trasmissione, inoltro, riproduzione, archiviazione e facilità di ricerca (quantomeno rispetto ad una raccomandata tradizionale);
- possibilità di invio multiplo, cioè a più destinatari contemporaneamente, (e verosimilmente con costi molto più bassi rispetto a quelli della raccomandata);
- tracciabilità della casella mittente e quindi del suo titolare;
- velocità della consegna (tipica anche dell'e-mail);
- possibilità di consultazione ed uso anche da postazioni diverse da quella del proprio ufficio o abitazione (basta un qualsiasi dispositivo, non solo PC, connesso ad Internet e un normale browser web) ed in qualunque momento, grazie alla persistenza del messaggio nella casella di posta elettronica;

- elevati requisiti di qualità e continuità del servizio;
- applicazione delle procedure atte a garantire la privacy dei dati personali nonché la sicurezza;
- garanzia dell'identità del mittente (titolare della casella).

Si comprende, quindi, come la PEC costituisca oggi un servizio che presenta indiscutibili vantaggi rispetto ai canali di comunicazione più tradizionali. A riguardo, di seguito si riporta un schema che sintetizza i principali vantaggi della PEC nei confronti delle principali modalità di comunicazione/spedizione (e-mail tradizionale, fax, posta e consegna *brevi manu*).

Gli ambiti di applicazione del servizio di PEC

Il mercato della PEC va quindi probabilmente ben al di là di quello oggi costituito dalla tradizionale raccomandata (con o senza ricevuta di ritorno). È infatti uno strumento in grado di intercettare le esigenze di una domanda significativa (ancora in gran parte potenziale) costituita da quanti utilizzano - per motivi di tempi/costi/semplicità - l'e-mail tradizionale per effettuare tutta una serie di comunicazioni, ma che gradirebbero (o necessiterebbero) avere al tempo stesso una certificazione della consegna del messaggio, dei suoi contenuti e di eventuali allegati. In tal senso, la PEC costituisce uno strumento in grado di rispondere non soltanto alle esigenze della *business community* e della Pubblica



Amministrazione ma anche a quelle dell'utente privato/cittadino e delle stesse famiglie (vedi schema).
Di seguito si riportano alcuni esempi concreti di comunicazione tra i diversi target individuati che possono essere veicolati attraverso la PEC. Per comodità d'esposizione si distinguono tre casi: Pubblica Amministrazione, aziende e privati.

Pubblica Amministrazione

Per quanto riguarda i vantaggi per la PA le indicazioni contenute nelle norme sono orientate a ridurre considerevolmente le voci di spesa relative all'utilizzo della posta tradizionale.
Oltre al contenimento della spesa i vantaggi aumentano considerevolmente se la PEC entra in un flusso di gestione documentale automatizzato. Ulteriori vantaggi derivanti alla PA dall'utilizzo della PEC sono la diminuzione dei contenziosi, in merito alla ricezione e invio di documenti e la consistente riduzione dei tempi delle pratiche.

Business community

Per quanto riguarda le comunicazioni B2B, le aziende possono utilizzare la PEC con i propri fornitori, clienti, partner, canali di vendita ecc., per comunicazioni sia di tipo economico (ad esempio, l'invio di fatture) e/o di tipo giuridico (ad esempio, per invio di un contratto). Basti pensare alle diverse forme di comunicazione che oggi attivano le banche (es. invio estratti conto), le assicurazioni o le utilities per la consegna di contratti e delle utenze. Tutte queste tipologie di comunicazione potranno migrare sulla PEC con un significativo risparmio di costi e tempi da parte dell'azienda mittente, ma anche con una serie di indubbi vantaggi per il cittadino, tra i quali si possono ricordare la facilità di consultazione da ogni luogo in cui sia accessibile internet, la possibilità di archiviare e ricercare i documenti, la possibilità di ottenere una riduzione dei costi dei singoli contratti.
Anche le relazioni/transazioni delle aziende con la PA sono largamente interessate, ad esempio si può ipotizzare l'invio alla Camera di Commercio di comunicazioni sociali (variazioni dello statuto e degli Organi sociali), la consegna dei bandi di gara, la richiesta di atti/certificati, ecc. Allo stesso modo potranno essere interessati i rapporti con INAIL, INPS

e i Fondi di previdenza. Altra applicazione che potrebbe ad esempio essere interessata è costituita dalla trasmissione degli F24 alle banche.
Anche gli studi professionali possono trarre vantaggio dall'utilizzo della PEC per tutte le transazioni e comunicazioni nei confronti sia delle amministrazioni pubbliche che dei propri clienti. Si pensi, ad esempio, che uno studio legale potrà veicolare sulla PEC le comunicazioni con la Cancelleria del Tribunale, le Prefetture, ecc.
A ciò si aggiunga l'interesse che possono avere le aziende a veicolare attraverso posta certificata tutta una serie di comunicazioni di rilievo ma che oggi sono trasmesse per posta tradizionale poiché il rapporto tra il costo di uno strumento più efficiente ed il costo del rischio risulta sfavorevole.

Comunicazioni del cittadino/famiglia

Anche il singolo cittadino può essere interessato ad attivare una propria casella di posta certificata in quanto, come più volte evidenziato, facilita, velocizza e rende meno costosa le comunicazioni nei confronti della PA, ad esempio per la richiesta di certificati, la contestazione delle multe, ed in generale la gestione dei rapporti con le aziende erogatrici servizi (banche, assicurazioni e utilities), si pensi, ad esempio, al caso di contenziosi, invio di reclami/contestazioni, ecc.
La possibilità inoltre di avere a disposizione, stando nella propria casa o perfino in vacanza, uno strumento in grado di effettuare e ricevere comunicazioni a valore legale di qualsiasi tipo con qualunque file digitale allegato consente un notevole livello di indipendenza e libertà di movimento.

Decreto del Presidente della Repubblica 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. 28 marzo 2005, n. 97

IL PRESIDENTE DELLA REPUBBLICA

- Visto l'articolo 87 della Costituzione;
- Visto l'articolo 15, comma 2, della legge 15 marzo 1997, n. 59;
- Visto l'articolo 27, commi 8, lettera e), e 9, della legge 16 gennaio 2003, n. 3;
- Visto l'articolo 17, comma 2, della legge 23 agosto 1988, n. 400;
- Visto l'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione del 25 marzo 2004;
- Espletata la procedura di informazione di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata con legge 21 giugno 1986, n. 317, così come modificata dal decreto legislativo 23 novembre 2000, n. 427;
- Acquisito il parere della Conferenza unificata, ai sensi dell'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, espresso nella riunione del 20 maggio 2004;
- Vista la nota del 29 marzo 2004, con la quale è stato richiesto il parere del Garante per la protezione dei dati personali;
- Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 14 giugno 2004;
- Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

- Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 28 gennaio 2005;
- Sulla proposta del Ministro per la funzione pubblica e del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze.

Emana il seguente regolamento:

Articolo 1
Oggetto e definizioni

Il presente regolamento stabilisce le caratteristiche e le modalità per l'erogazione e la fruizione di servizi di trasmissione di documenti informatici mediante posta elettronica certificata.

1. Ai fini del presente regolamento si intende per:
   a. BUSTA DI TRASPORTO, il documento informatico che contiene il messaggio di posta elettronica certificata;
   b. CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE, di seguito denominato: "CNIPA", l'organismo di cui all'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, come modificato dall'articolo 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196;
   c. DATI DI CERTIFICAZIONE, i dati inseriti nelle ricevute indicate dal presente regolamento, relativi alla trasmissione del messaggio di posta elettronica certificata;
   d. DOMINIO DI POSTA ELETTRONICA CERTIFICATA, l'insieme di tutte e sole le caselle di posta elettronica certificata il cui indirizzo fa riferimento, nell'estensione, ad uno stesso dominio della rete Internet, definito secondo gli standard propri di tale rete;
   e. LOG DEI MESSAGGI, il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal Gestore;
   f. MESSAGGIO DI POSTA ELETTRONICA CERTIFICATA, un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;
   g. POSTA ELETTRONICA CERTIFICATA, ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici;

h. POSTA ELETTRONICA, un sistema elettronico di trasmissione di documenti informatici;

i. RIFERIMENTO TEMPORALE, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;

l. UTENTE DI POSTA ELETTRONICA CERTIFICATA, la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi ente, associazione o organismo, nonché eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di posta elettronica certificata;

m. VIRUS INFORMATICO, un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Articolo 2
Soggetti del servizio di posta elettronica certificata

1. Sono soggetti del servizio di posta elettronica certificata:
   a. il mittente, cioè l'utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici;
   b. il destinatario, cioè l'utente che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici;
   c. il gestore del servizio, cioè il soggetto, pubblico o privato, che eroga il servizio di posta elettronica certificata e che gestisce domini di posta elettronica certificata.

Articolo 3
Trasmissione del documento informatico

1. Il comma 1 dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:
   "1. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi

dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.".

Articolo 4
Utilizzo della posta elettronica certificata

1. La posta elettronica certificata consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge.

2. Per i privati che intendono utilizzare il servizio di posta elettronica certificata, il solo indirizzo valido, ad ogni effetto giuridico, è quello espressamente dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni o di ogni singolo rapporto intrattenuto tra privati o tra questi e le pubbliche amministrazioni. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.

3. La volontà espressa ai sensi del comma 2 non può comunque dedursi dalla mera indicazione dell'indirizzo di posta certificata nella corrispondenza o in altre comunicazioni o pubblicazioni del soggetto.

4. Le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.

5. Le modalità attraverso le quali il privato comunica la disponibilità all'utilizzo della posta elettronica certificata, il proprio indirizzo di posta elettronica certificata, il mutamento del medesimo o l'eventuale cessazione della disponibilità, nonché le modalità di conservazione, da parte dei gestori del servizio, della documentazione relativa sono definite nelle regole tecniche di cui all'articolo 17.

6. La validità della trasmissione e ricezione del messaggio di posta elettronica certificata è attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna, di cui all'articolo 6.

7. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono di uno dei gestori di cui agli articoli 14 e 15.

Articolo 5
Modalità della trasmissione e interoperabilità

1. Il messaggio di posta elettronica certificata inviato dal mittente al proprio gestore di posta elettronica certificata viene da quest'ultimo trasmesso al

destinatario direttamente o trasferito al gestore di posta elettronica certificata di cui si avvale il destinatario stesso; quest'ultimo gestore provvede alla consegna nella casella di posta elettronica certificata del destinatario.

2. Nel caso in cui la trasmissione del messaggio di posta elettronica certificata avviene tra diversi gestori, essi assicurano l'interoperabilità dei servizi offerti, secondo quanto previsto dalle regole tecniche di cui all'articolo 17.

Articolo 6

Ricevuta di accettazione e di avvenuta consegna

1. Il gestore di posta elettronica certificata utilizzato dal mittente fornisce al mittente stesso la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata.

2. Il gestore di posta elettronica certificata utilizzato dal destinatario fornisce al mittente, all'indirizzo elettronico del mittente, la ricevuta di avvenuta consegna.

3. La ricevuta di avvenuta consegna fornisce al mittente prova che il suo messaggio di posta elettronica certificata è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica il momento della consegna tramite un testo, leggibile dal mittente, contenente i dati di certificazione.

4. La ricevuta di avvenuta consegna può contenere anche la copia completa del messaggio di posta elettronica certificata consegnato secondo quanto specificato dalle regole tecniche di cui all'articolo 17.

5. La ricevuta di avvenuta consegna è rilasciata contestualmente alla consegna del messaggio di posta elettronica certificata nella casella di posta elettronica messa a disposizione del destinatario dal gestore, indipendentemente dall'avvenuta lettura da parte del soggetto destinatario.

6. La ricevuta di avvenuta consegna è emessa esclusivamente a fronte della ricezione di una busta di trasporto valida secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

7. Nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati, le informazioni di cui all'articolo 11, detenute dai gestori, sono opponibili ai terzi ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Articolo 7
Ricevuta di presa in carico

1. Quando la trasmissione del messaggio di posta elettronica certificata avviene tramite più gestori il gestore del destinatario rilascia al gestore del mittente la ricevuta che attesta l'avvenuta presa in carico del messaggio.

Articolo 8
Avviso di mancata consegna

1. Quando il messaggio di posta elettronica certificata non risulta consegnabile il gestore comunica al mittente, entro le ventiquattro ore successive all'invio, la mancata consegna tramite un avviso secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

Articolo 9
Firma elettronica delle ricevute e della busta di trasporto

1. Le ricevute rilasciate dai gestori di posta elettronica certificata sono sottoscritte dai medesimi mediante una firma elettronica avanzata ai sensi dell'articolo 1, comma 1, lettera dd), del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata, che consente di rendere manifesta la provenienza, assicurare l'integrità e l'autenticità delle ricevute stesse secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

2. La busta di trasporto è sottoscritta con una firma elettronica di cui al comma 1 che garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

Articolo 10
Riferimento temporale

1. Il riferimento temporale e la marca temporale sono formati in conformità a quanto previsto dalle regole tecniche di cui all'articolo 17.

2. I gestori di posta elettronica certificata appongono un riferimento temporale su ciascun messaggio e quotidianamente una marca temporale sui log dei messaggi.

Articolo 11
Sicurezza della trasmissione

1. 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.

2. Durante le fasi di trasmissione del messaggio di posta elettronica certificata, i gestori mantengono traccia delle operazioni svolte su un apposito log dei messaggi. I dati contenuti nel suddetto registro sono conservati dal gestore di posta elettronica certificata per trenta mesi.

3. Per la tenuta del registro i gestori adottano le opportune soluzioni tecniche e organizzative che garantiscano la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni in esso contenute.

4. I gestori di posta elettronica certificata prevedono, comunque, l'esistenza di servizi di emergenza che in ogni caso assicurano il completamento della trasmissione ed il rilascio delle ricevute.

Articolo 12
Virus informatici

1. Qualora il gestore del mittente riceva messaggi con virus informatici è tenuto a non accettarli, informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione; in tale caso il gestore conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.

2. Qualora il gestore del destinatario riceva messaggi con virus informatici è tenuto a non inoltrarli al destinatario, informando tempestivamente il gestore del mittente, affinché comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione; in tale caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.

Articolo 13
Livelli minimi di servizio

1. I gestori di posta elettronica certificata sono tenuti ad assicurare il livello minimo di servizio previsto dalle regole tecniche di cui all'articolo 17.

Articolo 14
Elenco dei gestori di posta elettronica certificata

1. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono dei gestori inclusi in un apposito elenco pubblico disciplinato dal presente articolo.

2. Le pubbliche amministrazioni ed i privati che intendono esercitare l'attività di gestore di posta elettronica certificata inviano al CNIPA domanda di iscrizione nell'elenco dei gestori di posta elettronica certificata.

3. I richiedenti l'iscrizione nell'elenco dei gestori di posta elettronica certificata diversi dalle pubbliche amministrazioni devono avere natura giuridica di società di capitali e capitale sociale interamente versato non inferiore a un milione di euro.

4. I gestori di posta elettronica certificata o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione devono, inoltre, possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.

5. Non possono rivestire la carica di rappresentante legale, di componente del consiglio di amministrazione, di componente del collegio sindacale, o di soggetto comunque preposto all'amministrazione del gestore privato coloro i quali sono stati sottoposti a misure di prevenzione, disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423, e della legge 31 maggio 1965, n. 575, e successive modificazioni, ovvero sono stati condannati con sentenza irrevocabile, salvi gli effetti della riabilitazione, alla reclusione non inferiore ad un anno per delitti contro la Pubblica Amministrazione, in danno di sistemi informatici o telematici, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, ovvero per un delitto in materia tributaria.

6. Il richiedente deve inoltre:
   a. dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio di posta elettronica certificata;
   b. impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia della posta elettronica e della dimestichezza con procedure di sicurezza appropriate;

c. rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 17;

d. applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;

e. utilizzare per la firma elettronica, di cui all'articolo 9, dispositivi che garantiscono la sicurezza delle informazioni gestite in conformità a criteri riconosciuti in ambito europeo o internazionale;

f. adottare adeguate misure per garantire l'integrità e la sicurezza del servizio di posta elettronica certificata;

g. prevedere servizi di emergenza che assicurano in ogni caso il completamento della trasmissione;

h. fornire, entro i dodici mesi successivi all'iscrizione nell'elenco dei gestori di posta elettronica certificata, dichiarazione di conformità del proprio sistema di qualità alle norme ISO 9000, successive evoluzioni o a norme equivalenti, relativa al processo di erogazione di posta elettronica certificata;

i. fornire copia di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi.

7. Trascorsi novanta giorni dalla presentazione, la domanda si considera accolta qualora il CNIPA non abbia comunicato all'interessato il provvedimento di diniego.

8. Il termine di cui al comma 7 può essere interrotto una sola volta esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

9. Il procedimento di iscrizione nell'elenco dei gestori di posta elettronica certificata di cui al presente articolo può essere sospeso nei confronti dei soggetti per i quali risultano pendenti procedimenti penali per delitti in danno di sistemi informatici o telematici.

10. I soggetti di cui al comma 1 forniscono i dati, previsti dalle regole tecniche di cui all'articolo 17, necessari per l'iscrizione nell'elenco dei gestori.

11. Ogni variazione organizzativa o tecnica concernente il gestore ed il servizio di posta elettronica certificata è comunicata al CNIPA entro il quindicesimo giorno.

12. Il venire meno di uno o più requisiti tra quelli indicati al presente articolo è causa di cancellazione dall'elenco.

13. Il CNIPA svolge funzioni di vigilanza e controllo sull'attività esercitata dagli iscritti all'elenco di cui al comma 1.

Articolo 15
Gestori di posta elettronica certificata stabiliti nei Paesi dell'Unione europea

1. Può esercitare il servizio di posta elettronica certificata il gestore del servizio stabilito in altri Stati membri dell'Unione europea che soddisfi, conformemente alla legislazione dello Stato membro di stabilimento, formalità e requisiti equivalenti ai contenuti del presente decreto e operi nel rispetto delle regole tecniche di cui all'articolo 17. È fatta salva in particolare, la possibilità di avvalersi di gestori stabiliti in altri Stati membri dell'Unione europea che rivestono una forma giuridica equipollente a quella prevista dall'articolo 14, comma 3.

2. Per i gestori di posta elettronica certificata stabiliti in altri Stati membri dell'Unione europea il CNIPA verifica l'equivalenza ai requisiti ed alle formalità di cui al presente decreto e alle regole tecniche di cui all'articolo 17.

Articolo 16
Disposizioni per le pubbliche amministrazioni

1. Le pubbliche amministrazioni possono svolgere autonomamente l'attività di gestione del servizio di posta elettronica certificata, oppure avvalersi dei servizi offerti da altri gestori pubblici o privati, rispettando le regole tecniche e di sicurezza previste dal presente regolamento.

2. L'utilizzo di caselle di posta elettronica certificata rilasciate a privati da pubbliche amministrazioni incluse nell'elenco di cui all'articolo 14, comma 2, costituisce invio valido ai sensi del presente decreto limitatamente ai rapporti intrattenuti tra le amministrazioni medesime ed i privati cui sono rilasciate le caselle di posta elettronica certificata.

3. Le pubbliche amministrazioni garantiscono ai terzi la libera scelta del gestore di posta elettronica certificata.

4. Le disposizioni di cui al presente regolamento non si applicano all'uso degli strumenti informatici e telematici nel processo civile, nel processo penale, nel processo amministrativo, nel processo tributario e nel processo di-

nanzi alle sezioni giurisdizionali della Corte dei conti, per i quali restano ferme le specifiche disposizioni normative.

Articolo 17
Regole tecniche

1. Il Ministro per l'innovazione e le tecnologie definisce, ai sensi dell'articolo 8, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sentito il Ministro per la funzione pubblica, le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata. Qualora le predette regole riguardino la certificazione di sicurezza dei prodotti e dei sistemi è acquisito il concerto del Ministro delle comunicazioni.

Articolo 18
Disposizioni finali

1. Le modifiche di cui all'articolo 3 apportate all'articolo 14, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, (Testo A) si intendono riferite anche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 444 (Testo C). Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 11 febbraio 2005

CIAMPI
Berlusconi, Presidente del Consiglio dei Ministri
Baccini, Ministro per la funzione pubblica
Stanca, Ministro per l'innovazione e le tecnologie
Siniscalco, Ministro dell'economia e delle finanze

Visto, il Guardasigilli: Castelli

Registrato alla Corte dei conti il 18 aprile 2005
Registro n. 4, Ministeri istituzionali, foglio n. 332

Decreto 2 novembre 2005

Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata

G.U. 15 novembre 2005, n. 266

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

- Visto l'articolo 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, concernente
- Visto il Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- Visti gli articoli 8, comma 2, e 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante Testo unico sulla documentazione amministrativa, e successive modificazioni;
- Visto il decreto del Presidente del Consiglio dei Ministri 6 maggio 2005, concernente delega di funzioni del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie al Ministro senza portafoglio, dott. Lucio Stanca;
- Espletata la procedura di notifica alla Commissione europea, di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio del 20 luglio 1998, recepita nell'ordinamento italiano con il decreto legislativo 23 novembre 2000, n. 427;
- Sentito il Ministro per la funzione pubblica;

DECRETA

Capo I - Principi generali

Articolo 1
Definizioni

1. Ai fini del presente decreto si applicano le definizioni contenute nell'ar-

ticolo 1 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, citato nelle premesse. Si intende, inoltre, per:

a. punto di accesso: il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto;
b. punto di ricezione: il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto;
c. punto di consegna: il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna;
d. firma del gestore di posta elettronica certificata: la firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore;
e. ricevuta di accettazione: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata;
f. avviso di non accettazione: l'avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario;
g. ricevuta di presa in carico: la ricevuta, sottoscritta con la firma del

gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce;

h. ricevuta di avvenuta consegna: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario;
i. ricevuta completa di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale;
l. l) ricevuta breve di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale;
m. ricevuta sintetica di avvenuta consegna: la ricevuta che contiene i dati di certificazione;
n. avviso di mancata consegna: l'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario;
o. messaggio originale: il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene;
p. busta di trasporto: la busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione;
q. busta di anomalia: la busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia;
r. dati di certificazione: i dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore

di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto;

s. gestore di posta elettronica certificata: il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari;

t. titolare: il soggetto a cui è assegnata una casella di posta elettronica certificata;

u. dominio di posta elettronica certificata: dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata;

v. indice dei gestori di posta elettronica certificata: il sistema, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata.

z. casella di posta elettronica certificata: la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata;

aa. marca temporale: un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale del 27 aprile 2004, n. 98.

Articolo 2
Obiettivi e finalità

1. Il presente decreto definisce le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica certificata di cui al D.P.R. n. 68 del 2005.

Articolo 3
Norme tecniche di riferimento

1. Sono di seguito elencati gli standard di riferimento delle norme tecniche, le cui specifiche di dettaglio vengono riportate in allegato al presente decreto:
   a. RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted);
   b. RFC 1891 (SMTP Service Extension for Delivery Status Notifications);
   c. RFC 1912 (Common DNS Operational and Configuration Errors);
   d. RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions);
   e. RFC 2315 (PKCS #7: Cryptographic Message Syntax Version 1.5);
   f. RFC 2633 (S/MIME Version 3 Message Specification);
   g. RFC 2660 (The Secure HyperText Transfer Protocol);
   h. RFC 2821 (Simple Mail Transfer Protocol);
   i. RFC 2822 (Internet Message Format);
   l. RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification);
   m. RFC 3174 (US Secure Hash Algorithm 1 - SHA1);
   n. RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security);
   o. RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile).

Articolo 4
Compatibilità operativa degli standard

1. Il Centro nazionale per l'informatica nella Pubblica Amministrazione, di seguito denominato CNIPA, verifica, in funzione dell'evoluzione tecnologica, la coerenza operativa degli standard così come adottati nelle specifiche tecniche, dando tempestiva informazione delle eventuali variazioni nel proprio sito istituzionale.

Capo II - Disposizioni per i titolari e per i gestori di posta elettronica certificata

Articolo 5
Comunicazione e variazione della disponibilità all'utilizzo della posta elettronica certificata

2. La dichiarazione di cui all'articolo 4, comma 4, del D.P.R. n. 68 del 2005, può essere resa mediante l'utilizzo di strumenti informatici, nel qual caso la dichiarazione deve essere sottoscritta con la firma digitale di cui all'art. 1, comma 1, lettera n) del D.P.R. n. 445 del 2000.

3. La dichiarazione di cui al comma 1 è resa anche nei casi di variazione dell'indirizzo di posta elettronica certificata o di cessazione della volontà di avvalersi della posta elettronica certificata medesima.

Articolo 6
Caratteristiche dei messaggi gestiti dai sistemi di posta elettronica certificata

1. I sistemi di posta elettronica certificata generano messaggi conformi allo standard internazionale S/MIME, così come descritto dallo standard RFC 2633.

2. I messaggi di cui al comma 1 si dividono in tre categorie:
   a. ricevute;
   b. avvisi;
   c. buste.

3. La differenziazione dei messaggi, come indicato nel comma 2, è realizzata dai sistemi di posta elettronica certificata utilizzando la struttura header, prevista dallo standard S/MIME, da impostare per ogni tipologia di messaggio in conformità a quanto previsto dalle specifiche tecniche di cui all'allegato.

4. I sistemi di posta elettronica certificata in relazione alla tipologia di messaggio da gestire realizzano funzionalità distinte e specifiche.

5. L'elaborazione dei messaggi di posta elettronica certificata avviene anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di posta elettronica certificata.

6. Le ricevute generate dai sistemi di posta elettronica certificata sono le seguenti:

a. ricevuta di accettazione;
b. ricevuta di presa in carico;
c. ricevuta di avvenuta consegna completa, breve, sintetica.

7. La ricevuta di avvenuta consegna è rilasciata per ogni destinatario al quale il messaggio è consegnato.

8. Gli avvisi generati dai sistemi di posta elettronica certificata sono i seguenti:

a. avviso di non accettazione per eccezioni formali ovvero per virus informatici;
b. avviso di rilevazione di virus informatici;
c. avviso di mancata consegna per superamento dei tempi massimi previsti ovvero per rilevazione di virus informatici.

9. Le buste generate dai sistemi di posta elettronica certificata sono le seguenti:

a. busta di trasporto;
b. busta di anomalia.

10. La busta di trasporto è consegnata immodificata nella casella di posta elettronica certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente.

Articolo 7
Firma elettronica dei messaggi di posta elettronica certificata

1. I messaggi di cui all'articolo 6, generati dai sistemi di posta elettronica certificata, sono sottoscritti dai gestori mediante la firma del gestore di posta elettronica certificata, in conformità a quanto previsto dall'allegato.

2. I certificati di firma di cui al comma 1 sono rilasciati dal CNIPA al gestore al momento dell'iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata e sino ad un numero massimo di dieci firme per ciascun gestore.

3. Qualora un gestore abbia ravvisato la necessità di utilizzare un numero di certificati di firma superiore a dieci, può richiederli al CNIPA documentando tale necessità. Il CNIPA, previa valutazione della richiesta, stabilisce se fornire o meno al gestore ulteriori certificati di firma.

Articolo 8
Interoperabilità

1. Le specifiche tecniche finalizzate a garantire l'interoperabilità sono definite nell'allegato.

Articolo 9
Riferimento temporale

1. A ciascuna trasmissione è apposto un unico riferimento temporale, secondo le modalità indicate nell'allegato.

2. Il riferimento temporale può essere generato con qualsiasi sistema che garantisca stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala di Tempo Universale Coordinato (UTC), determinata ai sensi dell'articolo 3, comma 1, della legge 11 agosto 1991, n. 273.

Articolo 10
Conservazione dei log dei messaggi

1. Al fine della conservazione dei log dei messaggi, di cui alle deliberazioni del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico, ogni gestore provvede a:
   a. definire un intervallo temporale unitario non superiore alle ventiquattro ore;
   b. eseguire senza soluzioni di continuità il salvataggio dei log dei messaggi generati in ciascun intervallo temporale come sopra definito.
2. Ai file generati da ciascuna operazione di salvataggio deve essere associata la relativa marca temporale.

Articolo 11
Conservazione dei messaggi contenenti virus
e relativa informativa al mittente

1. Il gestore è tenuto a trattare il messaggio contenente virus secondo le regole tecniche indicate nell'allegato.

2. Il gestore è tenuto ad informare il mittente che il messaggio inviato contiene virus.

3. Il gestore è tenuto a conservare il messaggio contenente virus per un periodo non inferiore ai trenta mesi secondo le modalità indicate nelle delibe-

razioni del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico.

Articolo 12
Livelli di servizio

1. Il gestore di posta elettronica certificata può fissare il numero massimo di destinatari e la dimensione massima del singolo messaggio, sia per i messaggi che provengono da un suo titolare, sia per i messaggi che provengono da titolari di caselle di altri gestori di posta elettronica certificata.

2. In ogni caso il gestore di posta elettronica certificata deve garantire la possibilità dell'invio di un messaggio:
   a. almeno fino a cinquanta destinatari;
   b. per il quale il prodotto del numero dei destinatari per la dimensione del messaggio stesso non superi i trenta megabytes.

3. La disponibilità nel tempo del servizio di posta elettronica certificata deve essere maggiore o uguale al 99,8% del periodo temporale di riferimento.

4. Il periodo temporale di riferimento, per il calcolo della disponibilità del servizio di posta elettronica certificata, è pari ad un quadrimestre.

5. La durata massima di ogni evento di indisponibilità del servizio di posta elettronica certificata deve essere minore, o uguale, al 50% del totale previsto per l'intervallo di tempo di riferimento.

6. Nell'ambito dell'intervallo di disponibilità di cui al comma 3, la ricevuta di accettazione deve essere fornita al mittente entro un termine, da concordarsi tra gestore e titolare, da calcolare a partire dall'inoltro del messaggio, non considerando i tempi relativi alla trasmissione.

7. Al fine di assicurare in ogni caso il completamento della trasmissione ed il rilascio delle ricevute, il gestore di posta elettronica certificata descrive nel manuale operativo, di cui all'articolo 23, le soluzioni tecniche ed organizzative che realizzano i servizi di emergenza, ai sensi di quanto previsto dall'articolo 11, comma 4, del D.P.R. n. 68 del 2005, e consentano il rispetto dei vincoli definiti nei commi 4 e 5 del presente articolo.

Articolo 13
Avvisi di mancata consegna

1. Qualora il gestore del mittente non abbia ricevuto dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di

presa in carico o di avvenuta consegna del messaggio inviato, comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio.

2. Qualora, entro ulteriori dodici ore, il gestore del mittente non abbia ricevuto la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio entro le 24 ore successive all'invio, così come previsto dal D.P.R. n. 68 del 2005.

Articoll 14
Norme di garanzia sulla natura della posta elettronica ricevuta

1. Il gestore di posta elettronica certificata del destinatario ha l'obbligo di segnalare a quest'ultimo se la posta elettronica in arrivo non è qualificabile come posta elettronica certificata, secondo quanto prescritto dal D.P.R. n. 68 del 2005, nonché dal presente decreto e relativo allegato.

2. I messaggi relativi all'invio e alla consegna di documenti attraverso la posta elettronica certificata sono rilasciati indipendentemente dalle caratteristiche e dal valore giuridico dei documenti trasmessi.

Articolo 15
Limiti di utilizzo

1. La Pubblica Amministrazione che intende iscriversi all'elenco dei gestori di posta elettronica certificata, di cui all'articolo 14 del D.P.R. n. 68 del 2005, è tenuta a presentare al CNIPA una relazione tecnica che illustri le misure adottate affinché l'utilizzo di caselle di posta elettronica rilasciate a privati dall'amministrazione medesima:
   a. costituisca invio valido ai sensi dell'articolo 16, comma 2, del D.P.R. n. 68 del 2005;
   b. avvenga limitatamente ai rapporti di cui al medesimo articolo 16, comma 2.

Articolo 16
Modalità di iscrizione all'elenco dei gestori di posta elettronica certificata

1. I soggetti che presentano domanda di iscrizione all'elenco pubblico, di cui all'articolo 14 del D.P.R. n. 68 del 2005, forniscono inoltre al CNIPA

le informazioni e i documenti di seguito indicati, anche su supporto elettronico, ad eccezione del documento di cui alla lettera e):

a. denominazione sociale;
b. sede legale;
c. sedi presso le quali è erogato il servizio;
d. rappresentante legale;
e. piano per la sicurezza, contenuto in busta sigillata;
f. manuale operativo di cui all'articolo 23;
g. dichiarazione di impegno al rispetto delle disposizioni del D.P.R. n. 68 del 2005;
h. dichiarazione di conformità ai requisiti previsti nel presente decreto e suo allegato;
i. relazione sulla struttura organizzativa.

2. I soggetti che rivestono natura giuridica privata trasmettono, inoltre, copia cartacea di una polizza assicurativa o di un certificato provvisorio impegnativo di copertura dei rischi dell'attività e dei danni causati a terzi, rilasciata da una società di assicurazioni abilitata ad esercitare nel campo dei rischi industriali, a norma delle vigenti disposizioni.

Articolo 17
Equivalenza dei requisiti dei gestori stranieri

1. Il gestore di posta elettronica certificata stabilito in altri Stati membri dell'Unione europea che si trovi nelle condizioni di cui all'articolo 15 del D.P.R. n. 68 del 2005 ed intenda esercitare il servizio di posta elettronica certificata in Italia, comunica in via preventiva al CNIPA tale intenzione ed ogni notizia utile al fine della verifica di cui al citato articolo 15. La comunicazione costituisce domanda di iscrizione nell'elenco di gestori di posta elettronica certificata; sono applicabili le disposizioni procedimentali di cui all'articolo14 del D.P.R. n. 68 del 2005.

Articolo 18
Indice ed elenco pubblico dei gestori di posta elettronica certificata

1. I gestori di posta elettronica certificata si attengono alle regole riportate nell'allegato per accedere all'indice dei gestori di posta elettronica certificata.

2. Il certificato elettronico, da utilizzare per la funzione di accesso di cui al comma 1, è rilasciato dal CNIPA al gestore al momento dell'iscrizione nell'elenco pubblico di cui all'articolo 14 del D.P.R. n. 68 del 2005.

3. L'elenco pubblico dei gestori di posta elettronica certificata tenuto dal CNIPA contiene, per ogni gestore, le seguenti indicazioni:
   a. denominazione sociale;
   b. sede legale;
   c. rappresentante legale;
   d. indirizzo internet;
   e. data di iscrizione all'elenco;
   f. data di cessazione ed eventuale gestore sostitutivo.

4. L'elenco pubblico è sottoscritto con firma digitale dal CNIPA, che lo rende disponibile per via telematica.

Articolo 19
Disciplina dei compiti del CNIPA

1. Il CNIPA definisce con circolari le modalità di inoltro della domanda e le modalità dell'esercizio dei compiti di vigilanza e controllo di cui all'articolo 14 del D.P.R. n. 68 del 2005.

Articolo 20
Sistema di qualità del gestore

1. Entro un anno dall'iscrizione del gestore all'elenco pubblico di cui all'articolo 14 del D.P.R n. 68 del 2005, il gestore medesimo fornisce copia della certificazione di conformità del proprio sistema di qualità alle norme UNI EN ISO 9001:2000 e successive evoluzioni relativamente a tutti i processi connessi al servizio di posta elettronica certificata.

2. Il manuale della qualità è depositato presso il CNIPA e reso disponibile presso il gestore.

Articolo 21
Organizzazione e funzioni del personale del certificatore

1. L'organizzazione del personale addetto al servizio di posta elettronica certificata prevede almeno la presenza di responsabili preposti allo svolgimento delle seguenti attività e funzioni:
   a. registrazione dei titolari;
   b. servizi tecnici;
   c. verifiche e ispezioni (auditing);
   d. sicurezza;
   e. sicurezza dei log dei messaggi;

f. sistema di riferimento temporale.

2. È possibile attribuire al medesimo soggetto più responsabilità tra quelle previste dalle lettere d), e) ed f).

Articolo 22
Requisiti di competenza ed esperienza del personale

1. Il personale cui sono attribuite le funzioni previste dall'articolo 21 deve aver maturato un'esperienza almeno quinquennale nelle attività di analisi, progettazione, commercializzazione e conduzione di sistemi informatici.

2. Per ogni aggiornamento apportato al sistema di posta elettronica certificata, il gestore eroga, alle figure professionali interessate, apposita attività di addestramento.

Articolo 23
Manuale operativo

1. Il manuale operativo definisce e descrive le procedure applicate dal gestore di posta elettronica certificata nello svolgimento della propria attività.

2. Il manuale operativo è depositato presso il CNIPA.

3. Il manuale contiene:
   a. i dati identificativi del gestore;
   b. i dati identificativi della versione del manuale operativo;
   c. l'indicazione del responsabile del manuale operativo;
   d. l'individuazione, l'indicazione e la definizione degli obblighi del gestore di posta elettronica certificata e dei titolari;
   e. la definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
   f. l'indirizzo del sito web del gestore ove sono pubblicate le informazioni relative ai servizi offerti;
   g. le modalità di protezione della riservatezza dei dati;
   h. le modalità per l'apposizione e la definizione del riferimento temporale.

Il presente decreto è inviato ai competenti organi di controllo ed è pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 2 novembre 2005

Il Ministro per l'innovazione e le tecnologie Stanca

Circolare 24 novembre 2005, n. 49

Modalità per la presentazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68

G.U. 5 dicembre 2005, n. 283

La presente circolare indica le modalità con le quali i soggetti, pubblici e privati - che intendono esercitare l'attività di gestori di posta elettronica certificata (PEC), ai sensi dell'art. 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, devono presentare domanda al Centro nazionale per l'informatica nella Pubblica Amministrazione (di seguito indicato "CNIPA").

1 - Modalità di presentazione delle domande

La domanda, sottoscritta dal legale rappresentante della Pubblica Amministrazione o della società richiedente, corredata dei relativi allegati, deve essere inviata, in plico chiuso con l'indicazione del mittente, al CNIPA, via Isonzo 21b - 00198 Roma. La consegna può avvenire tramite servizio pubblico, o privato, oppure a mano nelle ore d'ufficio (9 - 13 e 15 - 17) dei giorni feriali, dal lunedì al venerdì. In caso di consegna a mano, verrà data formale ricevuta di consegna del plico. In alternativa, la domanda può essere predisposta, per quanto applicabile, in formato elettronico, utilizzando la sottoscrizione con firma digitale, ed essere inviata alla casella di posta elettronica cnipadir@cert.cnipa.it
La domanda deve indicare:

a. la denominazione, o la ragione sociale;
b. la sede legale;
c. il rappresentante legale (nel caso in cui i rappresentanti legali sono più di uno, va indicato il nominativo di ciascuno di loro);

d. l'elenco dei documenti allegati.

È opportuno che in detta domanda siano indicati anche il nominativo e i recapiti (numeri telefonici, numeri di telefax, indirizzo di posta elettronica) di un referente cui rivolgersi in presenza di problematiche di minore importanza che possono essere risolte anche per le vie brevi.Al fine di dimostrare il possesso dei requisiti previsti dall'art. 14 del decreto del Presidente della Repubblica n. 68/2005 e di ottemperare a quanto previsto dagli articoli 16, 21, 22 e 23 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005, e fatta salva la facoltà di avvalersi delle dichiarazioni sostitutive previste dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante "Testo unico sulla documentazione amministrativa", nel seguito indicato "Testo unico", alla domanda devono essere allegati:

a. una copia autentica dell'atto costitutivo della società;
b. una copia dello statuto sociale aggiornato, rilasciato dalla competente Camera di commercio industria artigianato e agricoltura in data non anteriore a novanta giorni rispetto alla data di presentazione della domanda stessa;
c. il certificato di iscrizione nel registro delle imprese, con dicitura antimafia, rilasciato in data non anteriore a novanta giorni rispetto alla data di presentazione della domanda;
d. una dichiarazione rilasciata dall'organo preposto al controllo o dal soggetto incaricato della revisione contabile ai sensi della normativa vigente, in data non anteriore a trenta giorni rispetto alla data di presentazione della domanda, attestante l'entità del capitale sociale versato, nonché l'ammontare e la composizione del patrimonio netto;
e. un prospetto della situazione patrimoniale, predisposto e approvato dall'organo amministrativo, di data non anteriore a centottanta giorni rispetto a quella di presentazione della domanda (sono tenute a questo adempimento solo le società già operative);
f. una relazione dell'organo preposto al controllo, o del soggetto incaricato della revisione contabile, redatta ai sensi della normativa vigente, sulla situazione patrimoniale di cui alla lettera e);
g. documentazione equivalente a quella prevista ai punti precedenti, legalizzata ai sensi dell'art. 33 del Testo unico (sono tenute a questo adempimento le società costituite all'estero ed aventi sede in Italia);
h. un elenco nominativo che rechi l'indicazione del/dei rappresentante/i legale/i, dei componenti dell'organo di amministrazione e dell'organo

di controllo, nonché di eventuali altri soggetti preposti all'amministrazione, con l'individuazione dei relativi poteri. Ognuno dei suddetti soggetti dovrà risultare in possesso, all'atto della domanda, dei requisiti di onorabilità previsti dall'art. 14 del decreto del Presidente della Repubblica n. 68/2005, comprovati:

1. per i cittadini italiani residenti in Italia:
   aa. dalla dichiarazione sostitutiva di atto di notorietà;
   bb. dal certificato del casellario giudiziale;
   cc. dal certificato relativo ai carichi pendenti;
2. per le persone che non rientrano nella categoria di cui al precedente alinea:
   aa. dalla dichiarazione, resa davanti a pubblico ufficiale;
   bb. dai certificati attestanti che il soggetto non è fallito o sottoposto a procedura equivalente.

Le firme apposte sulla documentazione anzidetta devono esser legalizzate con le modalità previste dal citato Testo unico. In alternativa, per i soggetti iscritti nell'albo di cui all'art. 13 del decreto legislativo 1° settembre 1993, n. 385, recante: "Testo unico delle leggi in materia bancaria e creditizia", la dimostrazione del possesso dei requisiti di onorabilità potrà essere assolta mediante apposita dichiarazione sostitutiva di certificazione, resa ai sensi dell'art. 46 del testo unico dal legale rappresentante, comprovante l'iscrizione nel suddetto albo alla data di presentazione della domanda di iscrizione:

a. una copia della polizza assicurativa, o certificato provvisorio impegnativo, stipulata per la copertura dei rischi derivanti dall'attività e dagli eventuali danni causati a terzi, rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali a norma delle vigenti disposizioni;
b. una copia dell'ultimo bilancio, e relativa certificazione, se la società è stata costituita da più di un anno;
c. una dichiarazione, rilasciata dal presidente della società, attestante la composizione dell'azionariato, con l'indicazione, comunque, dei soggetti partecipanti, in forma diretta o indiretta, al capitale sociale medesimo, in misura superiore al 5%, nonché della data a cui si riferisce detta dichiarazione;
d. una copia del manuale operativo, redatto come indicato al successivo punto 2.1, sottoscritto da un soggetto munito di potere di firma;
e. una copia del piano per la sicurezza, redatto come indicato al successi-

vo punto 2.2, sottoscritto e siglato in ogni foglio da un soggetto munito di potere di firma;

f. una relazione sulla struttura organizzativa, debitamente sottoscritta dal legale rappresentante, che contenga, oltre all'elenco del personale addetto all'erogazione del servizio e dei compiti allo stesso affidati, l'indicazione:
   a. dei nomi dei responsabili delle attività di cui all'art. 21 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005;
   b. dei requisiti di competenza ed esperienza del personale di cui al punto precedente;
   c. dello specifico ruolo che il gestore svolge all'interno della struttura aziendale;
   d. della ripartizione delle varie mansioni svolte nella struttura organizzativa e delle connesse responsabilità;
g. una dichiarazione di piena disponibilità a consentire l'accesso di incaricati del CNIPA presso le strutture dedicate all'erogazione del servizio di posta elettronica certificata, al fine di poter verificare la rispondenza delle stesse ai requisiti tecnici, organizzativi e funzionali di cui alla documentazione allegata alla domanda;
h. una descrizione delle caratteristiche dei dispositivi sicuri utilizzati per la creazione della firma delle ricevute, degli avvisi e delle buste di trasporto. Le caratteristiche di sicurezza di detti dispositivi dovranno essere valutate secondo le specifiche CEN: CWA 14169. Sono altresì ammessi:
e. i livelli di valutazione E3 e robustezza HIGH dell'ITSEC e EAL 4 della norma ISO/IEC 15408 o superiori;
f. i livelli di valutazione internazionalmente riconosciuti;
g. i dispositivi previsti dalla normativa in materia di firma digitale;
i. una dichiarazione d'impegno a comunicare al CNIPA ogni eventuale variazione intervenuta rispetto a quanto dichiarato nella domanda di iscrizione. A seguito di tale comunicazione il CNIPA può procedere ad una nuova, se del caso anche parziale, valutazione dei requisiti o richiedere ulteriore documentazione;
j. una descrizione delle modalità operative del servizio, con riferimento all'implementazione delle regole tecniche (architettura tecnica e funzionale, indicazione dei principali prodotti/componenti software utilizzati).

I certificatori iscritti nell'elenco pubblico di cui all'art. 28, comma 1, del Testo unico sono esentati, in esito a specifica richiesta in tal senso, dalla presentazione della documentazione di cui alle lettere a), b), c), d), e), f),

h), l), m), purché in corso di validità, in quanto già prodotta in sede di accreditamento e disponibile presso il CNIPA.

2 - Requisiti tecnico-organizzativi

2.1 Manuale operativo

Il manuale operativo individua le regole generali e le procedure seguite dal gestore di posta elettronica certificata (PEC) nello svolgimento della propria attività ed è pubblicato a garanzia dell'affidabilità dei servizi offerti dal gestore stesso ai propri utenti e ai loro corrispondenti. Detto manuale è disponibile per la consultazione ed il download sul sito del gestore. Oltre ai dati identificativi della versione in uso alla quale si riferisce, il manuale operativo deve contenere, quanto meno:

a. i dati identificativi del gestore;
b. l'indicazione del responsabile del manuale stesso;
c. i riferimenti normativi necessari per la verifica dei contenuti;
d. l'indirizzo del sito web del gestore ove è pubblicato e scaricabile;
e. l'indicazione delle procedure nonché degli standard tecnologici e di sicurezza utilizzati dal gestore nell'erogazione del servizio;
f. le definizioni, le abbreviazioni e i termini tecnici che in esso figurano;
g. una descrizione sintetica del servizio offerto;
h. la descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi;
i. l'indicazione del contenuto e delle modalità dell'offerta da parte del gestore;
j. l'indicazione delle modalità di accesso al servizio;
k. l'indicazione dei livelli di servizio e dei relativi indicatori di qualità di cui all'art. 12 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005;
l. l'indicazione delle condizioni di fornitura del servizio;
m. l'indicazione delle modalità di protezione dei dati dei titolari;
n. l'indicazione degli obblighi e delle responsabilità che ne discendono, delle esclusioni e delle eventuali limitazioni, in sede di indennizzo, relative ai soggetti previsti all'art. 2 del decreto del Presidente della Repubblica n. 68/2005.

Il numero di pagine del manuale operativo deve essere compreso tra cinquanta (50) e cento (100); ogni pagina deve contenere, mediamente, quaranta (40) righe; la dimensione del carattere deve essere pari a dodici punti.
È data facoltà di limitare le dichiarazioni contenute nel manuale operativo alle sole informazioni non soggette a particolari ragioni di riservatezza.
Il CNIPA si riserva, comunque, a norma dell'art. 14, comma 8, del decreto del Presidente della Repubblica n. 68/2005, di richiedere integrazioni della documentazione presentata e di effettuare le opportune verifiche in merito a quanto dichiarato.

2.2 Piano per la sicurezza

Il piano per la sicurezza, corredato delle relative procedure attinenti all'organizzazione, in quanto documento riservato, deve essere inserito all'interno del plico contenente la domanda, in busta separata e sigillata da cui risulti la denominazione della Pubblica Amministrazione o la ragione sociale della società che richiede l'iscrizione e la dicitura "Piano per la sicurezza, versione del ...".
Il piano deve contenere, quanto meno:

a. una descrizione delle procedure utilizzate nell'erogazione del servizio (attivazione dell'utenza e organizzazione del servizio di posta elettronica certificata), con particolare riferimento ai problemi attinenti alla sicurezza, alla gestione dei log-file e alla garanzia della loro integrità;
b. una descrizione dei dispositivi di sicurezza installati;
c. una descrizione dei flussi di dati;
d. l'indicazione della procedura di gestione e conservazione delle copie di sicurezza dei dati;
e. l'indicazione della procedura da seguire al verificarsi di possibili guasti di grande rilevanza che determinino l'arresto del servizio (occorre precisare i tipi di guasti per i quali sono state previste delle soluzioni: calamità naturali, dolo, indisponibilità prolungata del sistema, o altri eventi) e descrizione delle soluzioni proposte per farvi fronte, con informazioni dettagliate circa i tempi e le modalità previste per il ripristino;
f. un'analisi dei rischi (occorre precisare le possibili tipologie di rischio: dolo, infedeltà del personale, inefficienza operativa, inadeguatezza tecnologica, o altro);
g. una descrizione delle procedure per la gestione dei rischi di cui al punto precedente (occorre precisare i tempi di reazione previsti e i nomi dei responsabili tenuti ad intervenire);

h. una dettagliata indicazione dei controlli previsti (occorre indicare, se è previsto, il ricorso periodico a ispezioni esterne);
i. l'indicazione della struttura generale e della struttura logistica dell'organizzazione e delle relative modalità operative;
j. una sommaria descrizione dell'infrastruttura di sicurezza per ciascun immobile di cui si compone la struttura;
k. una breve descrizione dell'allocazione degli impianti informatici, dei servizi e degli uffici collocati negli immobili che fanno parte della struttura;
l. l'indicazione delle modalità di tenuta dei log dei messaggi;
m. una descrizione della procedura di accesso ai log dei messaggi da parte del personale del gestore;
n. una descrizione del sistema di riferimento temporale e della marca temporale adottata;
o. una descrizione dei sistemi adottati per garantire la riservatezza e l'integrità delle trasmissioni di messaggi mediante il sistema.

I certificatori qualificati accreditati, iscritti nell'elenco pubblico tenuto dal CNIPA, potranno fare riferimento ai dati ed agli elementi contenuti nel piano della sicurezza già in possesso del CNIPA medesimo.

3 - Modalità di esame delle domande

L'istruttoria delle domande di iscrizione presentate, e la verifica della regolarità della relativa documentazione prodotta, sono effettuate, ai sensi del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005, dal CNIPA che, una volta conclusa l'istruttoria, adotta il conseguente provvedimento di accoglimento o di reiezione, ovvero, se ritenuta necessaria, si riserva di procedere ad una integrazione di istruttoria.
Il soggetto la cui domanda sia stata oggetto di un provvedimento di reiezione non può presentare una nuova istanza di iscrizione se non sono cessate le cause che hanno determinato, a suo tempo, il mancato accoglimento della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata.

Roma, 24 novembre 2005

Il presidente del Centro nazionale per l'informatica nella Pubblica Amministrazione Zoffoli

Centro nazionale per l'informatica nella Pubblica Amministrazione

Circolare 7 dicembre 2006, n. 51

Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 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. 21 dicembre 2006, n. 296

Premessa

L'art. 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3", attribuisce, tra l'altro, al Centro nazionale per l'informatica nella Pubblica Amministrazione (di seguito indicato "CNIPA"):

- la gestione dell'elenco pubblico di cui al medesimo art. 14 (di seguito indicato "elenco");
- il compito di procedere all'iscrizione nell'elenco dei soggetti in possesso dei requisiti prescritti.

Consequenziale alle richiamate funzioni, è l'attribuzione al CNIPA, ai sensi dell'art. 14, comma 13, del citato decreto del Presidente della Repubblica n. 68 del 2005, di funzioni di vigilanza e di controllo sull'attività esercitata dai soggetti iscritti nell'elenco, dalle quali discende altresì il compito di monitorare - anche in collaborazione con le autorità competenti - eventuali casi di esercizio o pubblicizzazione della attività di gestore di posta elettronica certificata (di seguito indicata "PEC") da parte di soggetti non abilitati.
Successivamente, l'art. 19 del decreto del Ministro per l'innovazione e le tecnologie D.M. 2 novembre 2005, recante "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata", ha demandato al CNIPA il compito di definire, con pro-

prie circolari, sia le modalità di inoltro delle domande di iscrizione nell'elenco, sia le modalità dell'esercizio dei richiamati compiti di vigilanza e controllo.
Il CNIPA, con la circolare 24 novembre 2005, n. CNIPA/CR/49, ha provveduto a fornire le indicazioni relative alle modalità con le quali coloro che intendono esercitare attività di gestori di PEC devono presentare domanda.
Con la presente circolare si indicano le modalità attraverso le quali il CNIPA svolge la suddetta funzione di vigilanza e di controllo.

1. Test di interoperabilità del sistema di gestione della PEC

1.1. Ai sensi dell'art. 5 del citato decreto del Presidente della Repubblica n. 68 del 2005 e dell'art. 8 del decreto del Ministro per l'innovazione e tecnologie del 2 novembre 2005 (di seguito indicato "decreto ministeriale"), i sistemi di PEC utilizzati dai gestori devono essere interoperabili.
Il CNIPA svolge la funzione di vigilanza e di controllo sulla predetta interoperabilità ai sensi dei successivi punti.

1.2 Ogni gestore deve superare con esito positivo una serie di test di interoperabilità presso una struttura indicata dal CNIPA. La serie di test è pubblicata sul sito del CNIPA (www.cnipa.gov.it). Detti test devono essere ripetuti ogni volta che il gestore apporti modifiche funzionali o tecniche che impattino sull'interoperabilità dei sistemi di PEC. Il gestore deve, in ogni caso, fornire al CNIPA una casella di PEC per tutto il periodo di esercizio della relativa attività.

1.3 I test di interoperabilità di cui al punto 1.2 sono obbligatori trascorso il termine di trenta giorni solari che decorrono dal giorno successivo a quello della loro pubblicazione sul sito del CNIPA. Quest'ultimo comunica a ciascun gestore la pianificazione delle rispettive fasi di test.

1.4 Il CNIPA può in qualsiasi momento effettuare verifiche, anche mediante visite presso il gestore, per accertare la piena interoperabilità del sistema di PEC del gestore medesimo, anche richiedendo la ripetizione, in tutto o in parte, della serie di test.

2. Vigilanza e controllo sull'esercizio delle attività dei gestori

2.1 Il CNIPA esercita attività di vigilanza e di controllo al fine di verificare il possesso e il mantenimento dei requisiti previsti per l'iscrizione nell'elenco.

3. Modalità di vendita dei servizi di PEC attraverso canali commerciali

3.1 Il CNIPA monitora le modalità di vendita dei servizi di PEC attraverso canali commerciali, anche avvalendosi del supporto di terzi, e verifica, in particolare, che le modalità di vendita siano conformi alle prescrizioni di legge e che il rapporto contrattuale sia sempre posto in essere tra il titolare di cui all'art. 1, lettera t) del decreto ministeriale ed un gestore; a tal fine, ogni gestore deve mettere a disposizione del CNIPA, su richiesta di quest'ultimo, le informazioni del caso.

4. Struttura informativa dei gestori

4.1 Il gestore organizza una struttura informativa che raccoglie e gestisce le informazioni relative:

a. al numero di caselle in esercizio per ciascun dominio;
b. al numero totale giornaliero di messaggi di PEC in ingresso alle caselle gestite ed in uscita dalle stesse;
c. ai livelli di servizio erogati, con riferimento a quelli previsti dal decreto ministeriale;
d. al numero totale giornaliero di virus rilevati in ingresso ai sistemi gestiti ed in uscita dagli stessi.

Le informazioni di cui alle lettere a), b), c), d) devono essere inviate al CNIPA con le modalità e nei tempi definiti al punto 5.

4.2 Il CNIPA può inoltre richiedere ai gestori:

a. informazioni circa il livello di soddisfazione dei propri clienti;
b. le caratteristiche di eventuali servizi aggiuntivi offerti.

4.3 In un'apposita sezione della struttura informativa sono registrate e gestite le informazioni relative a disservizi, segnalazioni e reclami secondo la classificazione riportata nell'allegata tabella "A".

5. Tempi e modalità delle comunicazioni dirette al CNIPA.

5.1 Ogni gestore è tenuto a raccogliere le informazioni di cui al punto 4.1 trascorso il termine di sessanta giorni solari decorrenti dalla data di pubblicazione della presente circolare.

Dette informazioni devono essere inviate al CNIPA con le cadenze di seguito indicate:

a. con frequenza bimestrale, entro il quindicesimo giorno successivo al termine del bimestre di riferimento, devono essere trasmesse le informazioni relative:
   - al numero di caselle in esercizio per ciascun dominio;
   - al numero totale giornaliero di messaggi di PEC in ingresso alle caselle gestite ed in uscita dalle stesse;
   - al numero totale giornaliero di virus rilevati in ingresso ai sistemi gestiti ed in uscita dagli stessi;

b. con frequenza quadrimestrale, entro il quindicesimo giorno successivo al termine del quadrimestre di riferimento, devono essere trasmesse le informazioni concernenti:
   - i livelli di servizio erogati, con riferimento a quelli previsti dal decreto ministeriale citato in premessa.

5.2 Le informazioni di cui al punto 5.1 devono essere inviate tramite posta elettronica certificata alla casella gestoripec@cert.cnipa.it. Le informazioni di cui alla lettera a) del punto 5.1 devono avere un formato conforme a quanto descritto nel sito del CNIPA. Le informazioni di cui alla lettera b) del punto 5.1 devono essere in formato Adobe PDF.

6. Segnalazioni urgenti al CNIPA di malfunzionamenti gravi

6.1 I gestori hanno l'obbligo di comunicare al CNIPA, con le modalità e nei tempi indicati al punto 6.2, i disservizi di cui al punto 4, contraddistinti da uno dei seguenti codici: 1A, 1B, 2A, 2B, 3A, 3B, secondo quanto riportato nell'allegata tabella "A".

6.2 In particolare, il gestore è tenuto ad informare il CNIPA dell'evento occorso, entro trenta minuti dalla rilevazione dell'evento stesso, utilizzando i recapiti e l'apposito modulo indicati nel sito del CNIPA medesimo. La comunicazione deve fornire anche una prima valutazione dell'incidente e le eventuali misure adottate al riguardo.

7. Sospensione del servizio

7.1 Nel caso di comportamento anomalo e non circoscritto (codici 1A e 1B della citata tabella "A"), il gestore è tenuto a sospendere il servizio, fornen-

do adeguata e tempestiva informativa ai propri utenti ed agli altri gestori. Ove il gestore coinvolto non attivi l'autosospensione, il CNIPA dispone la sospensione del servizio.

7.2 Nel caso di comportamento anomalo e circoscritto (codici 2A e 2B della citata tabella "A"), il CNIPA può disporre la sospensione del servizio per il gestore coinvolto, fino alla rimozione delle cause che hanno determinato detto comportamento anomalo e circoscritto; in tal caso, il gestore fornisce adeguata e tempestiva informativa ai propri utenti ed agli altri gestori.

7.3 Non appena ripristinata l'operatività, il gestore comunica al CNIPA l'avvenuta rimozione delle cause che hanno determinato il comportamento anomalo e fornisce parimenti al CNIPA entro una settimana dalla data della comunicazione di cui al presente punto, una circostanziata relazione tecnica sull'accaduto e sui provvedimenti adottati in conseguenza.

7.4 Il gestore attua l'autosospensione producendo un "avviso di non accettazione per eccezioni formali" relativamente ai messaggi immessi dai propri utenti e non producendo la "ricevuta di presa in carico" per i messaggi destinati ai propri utenti.

7.5 La sospensione del servizio disposta dal CNIPA viene attuata dal gestore con le medesime modalità previste per l'autosospensione.

7.6 Qualora il gestore coinvolto non ottemperi a quanto prescritto ai punti 7.1 e 7.2, il CNIPA può disporne la cancellazione dall'elenco.

8. Verifiche periodiche dei gestori

8.1 I gestori hanno l'obbligo di effettuare verifiche semestrali, i cui esiti sono riportati in relazioni sottoscritte dal responsabile delle verifiche stesse e delle ispezioni, come previsto dal decreto ministeriale, e messe a disposizione, su richiesta, del CNIPA. Dette verifiche devono riguardare, in particolare, le componenti tecniche ed organizzative del sistema di PEC, il sistema di raccolta dei livelli di servizio e le tipologie di contratti di vendita dei servizi di PEC.

9. Verifiche del CNIPA

9.1 Con riferimento alla dichiarazione di cui alla lettera q) del punto 1 della citata circolare n. CNIPA/CR/49 del 24 novembre 2005, il CNIPA può ef-

fettuare, con un preavviso di 48 ore, sopralluoghi presso le strutture utilizzate dal gestore per verificare la conformità del sistema di PEC.

10. Provvedimenti nei confronti dei gestori inadempienti

10.1 A seguito delle risultanze dell'attività di vigilanza e di controllo, nell'ipotesi di inosservanza di uno o più degli obblighi posti a carico del gestore, il CNIPA può disporre l'inibizione dell'esercizio dell'attività svolta dal gestore inadempiente, indicando nel contempo il termine entro il quale il gestore stesso deve conformarsi agli obblighi previsti. Qualora il gestore non provveda in tal senso nei tempi indicati, il CNIPA può disporre la cancellazione del gestore medesimo dall'elenco.

10.2 Nel caso in cui il CNIPA disponga la cancellazione di un gestore dall'elenco rimane in capo al gestore stesso l'obbligo di conservare e rendere disponibili, su richiesta, i log prodotti nell'ambito dell'attività svolta come previsto dall'art. 11, comma 2, del citato decreto del Presidente della Repubblica n. 68 del 2005.

Il Presidente
Zoffoli

Allegato

Tabella A
Classificazione dei disservizi in relazione agli effetti prodotti e relativi codici identificativi

1. **Comportamento anomalo e non circoscritto**: comportamento difforme dalle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, relativo alle funzioni base (trattamento del messaggio originario, ricevute e avvisi) per il quale non è circoscritto il potenziale impatto (codice 1A, se rilevato dal gestore; codice 1B, se rilevato da terzi).
2. **Comportamento anomalo circoscritto**: comportamento difforme dalle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, relativo alle funzioni base (trattamento del messaggio originario, ricevute e avvisi) per il quale è circoscritto il potenziale impatto (codice 2A, se rilevato dal gestore; codice 2B, se rilevato da terzi).
3. **Malfunzionamento bloccante**: tipologia di malfunzionamento a causa del quale le funzionalità del sistema di PEC, come definite nelle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, non possono essere utilizzate in tutto o in parte dagli utenti (codice 3A, se rilevato dal gestore; codice 3B, se rilevato da terzi).
4. **Malfunzionamento grave**: tipologia di malfunzionamento a causa del quale in alcune circostanze le funzionalità del sistema di PEC, come definite nelle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, non possono essere utilizzate in tutto o in parte dagli utenti (codice 4A, se rilevato dal gestore; codice 4B, se rilevato da terzi).
5. **Malfunzionamento**: situazione a causa della quale le funzionalità del sistema di PEC, come definite nelle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, in tutto o in parte, risultano degradate ovvero il sistema ha un comportamento anomalo in situazioni circoscritte e per funzionalità secondarie (esclusi: la procedura di identificazione, i messaggi originari, le ricevute, gli avvisi e le buste) (codice 5A, se rilevato dal gestore; codice 5B, se rilevato da terzi).

Classificazione dei reclami/segnalazioni degli utenti e relativi codici identificativi

RC Segnalazione di un reclamo relativo al rapporto contrattuale.

AL Segnalazione di un reclamo relativo alla procedura di accesso al log.

SA Segnalazione di anomalia/disservizio non imputabili al gestore (client, collegamento internet, gestione utenze decentrate).

COLLANA MINIGRAFIE CNIPA

- n. 1 “Legge Stanca e regolamento di attuazione”
- n. 2 “Legge Stanca: requisiti di accessibilità”
- n. 3 “La TV digitale terrestre: progetti per la PA”
- n. 4 “Scuola virtuale PA”
- n. 5 “Portale delle imprese”
- n. 6 “Protocollo ASP”
- n. 7 “Normativa italiana sull'accessibilità”
- n. 8 “La qualità dei beni e servi nei contratti della PA: LG per una migliore gestione”
- n. 9 “Cos’è il Cnipa”
- n. 10 “Continuità operativa nella PA”
- n. 11 “Posta elettronica certificata”
- n. 12 “Lotta agli sprechi”
- n. 13 “Codice Amministrazione digitale”
- n. 14 “La normativa sulla firma elettronica”
- n. 15 “Scuola virtuale PA” II edizione
- n. 16 “Il Sistema Pubblico di connettività: i consuntivi del primo periodo di attività”

Segreteria tecnica e Comunicazione
Pubblicazioni e sito Internet
comunicazione@cnipa.it
tel. 06 85264.207

via Isonzo, 21/b – 00198 Roma

www.cnipa.gov.it