Università degli studi di Perugia

Facoltà di scienze Matematiche Fisiche e Naturali

Corso di Laurea Magistrale in Informatica

Seminario di Sicurezza Informatica
Prof. Stefano Bistarelli

La PEC
Posta Elettronica Certificata

A cura di

Donati Gianni

La Pec

Cos'è la PEC

Pec è l'acronimo di **Posta Elettronica Certificata** ed è un sistema di posta elettronica mediante il quale è possibile inviare e ricevere documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici, avendo così lo stesso valore legale di una raccomandata con avviso di ricevimento.

Rappresenta un'evoluzione in termini di garanzie per la classica posta elettronica che di per sé non ha assolutamente nessun valore legale, fin dai suoi albori infatti ha rappresentato un semplice nonché rapido mezzo di comunicazione, che ha cambiato gli stili di comunicazione classica fino a quel momento utilizzati.

Vs

La **Posta Elettronica Certificata** permette di accelerare i contatti tra Pubbliche Amministrazioni e imprese rendendo più sicura ed economica la trasmissione documentale, infatti per le sue caratteristiche permette la trasmissione e la ricezione di messaggi in cui si possono avere le stesse caratteristiche di un messaggio di posta raccomandata classica, con tutti i vantaggi derivanti dall'uso della posta elettronica.

Quando e come

Lo standard Pec è prettamente italiano, infatti la Pec nasce in Italia nel 2005 attraverso una legge che attribuisce ad un organo preposto i compiti di gestione del servizio Pec, tale organo è chiamato CNIPA che è l'acronimo di Centro Nazionale per l'Informatizzazione della Pubblica Amministrazione.
Attualmente l'organo amministrativo competente risulta essere DigitPA, Pubblica Amministrazione digitale (tutti i compiti del CNIPA sono stati trasferiti al DigitPa), il quale si occupa appunto della modernizzazione della pubblica amministrazione attraverso l'implementazione dei sistemi digitali che consentono una più agevole fruibilità dei servizi.
DigitPA, all'interno del proprio sito istituzionale, rende disponibile una apposita sezione riguardante la posta elettronica certificata, contenente una versione scaricabile di tutta la documentazione valida

ai fini di legge e riguardante la PEC.

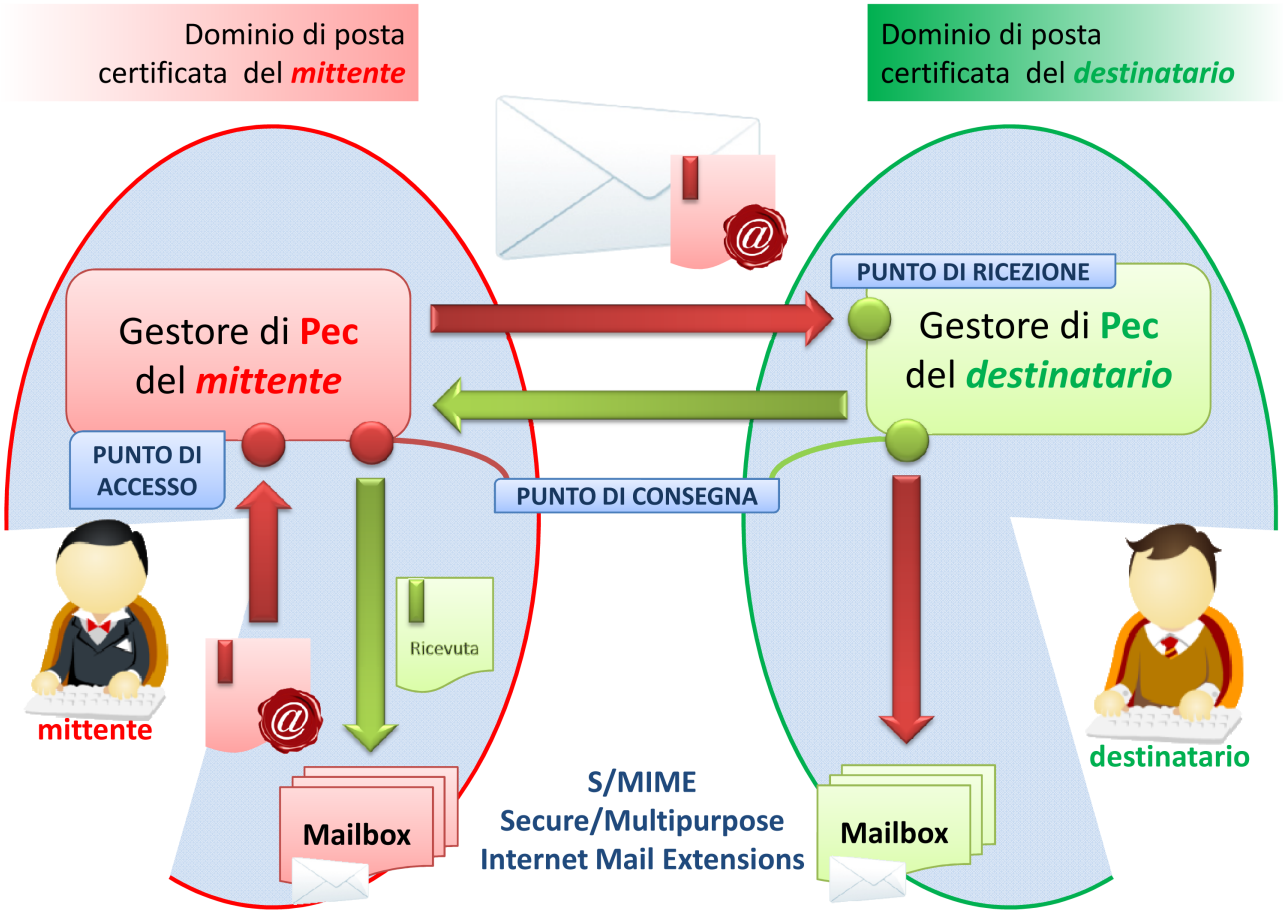
In particolar modo DigitPA si occupa di vagliare fra i fornitori che richiedono di poter fornire il servizio PEC; Infatti la Posta elettronica certificata può essere fornita solo dai cosiddetti fornitori accreditati, che vengono autorizzati a fornire il servizio proprio da DigitPA in base al rispetto dei canoni stabiliti per legge al fine di preservare tutte le caratteristiche del servizio, la normativa italiana richiede che una azienda, per diventare gestore del servizio PEC, debba superare una apposita procedura di accreditamento.

Nel caso in cui un gestore non offra i servizi di base atti a garantire il servizio Pec non verrà autorizzato a fornire il servizio stesso.

Come funziona la PEC

Il primo punto su cui si deve porre l'accento è il fatto che per il servizio di Posta Elettronica Certificata si devono usare solamente domini dedicati, cioè domini il cui compito esclusivo è quello di gestire la Pec. Pertanto non possono esistere domini promiscui che al contempo gestiscano la posta elettronica "classica", e la Pec; infatti se ciò accadesse risulterebbe più facile un'eventuale compromissione del servizio Pec.

Vediamo ora lo schema di funzionamento della Posta elettronica certificata:



I messaggi di posta certificata vengono spediti tra 2 caselle, e quindi Domini, certificati.

Alla trasmissione di un messaggio PEC partecipano diverse entità:

- Il mittente, che vuole inviare un messaggio PEC
- Il destinatario, al quale il mittente vuole recapitare il messaggio PEC
- Il gestore del mittente, che mantiene un rapporto contrattuale con il mittente per quanto riguarda i servizi PEC
- Il gestore del destinatario, che mantiene un rapporto contrattuale con il destinatario per quanto riguarda i servizi PEC
- La rete internet (più in generale la rete di comunicazione)
- Il messaggio PEC

Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato, accede per prima cosa attraverso la verifica delle credenziali di accesso (username e password) al **server di Posta Elettronica Certificata** del suo gestore, poi il processo di trasmissione di un messaggio PEC segue i seguenti passi:

- Il mittente predispone il messaggio PEC e lo sottopone al gestore mittente.
- Il gestore mittente verifica la correttezza formale del messaggio PEC e, in caso positivo, restituisce al mittente la ricevuta di accettazione come riconoscimento dell'avvenuto invio del messaggio. La ricevuta è firmata digitalmente dal gestore e garantisce l'integrità, e da un'eventuale rilevazione virus nell'intero messaggio con i suoi allegati
- Il gestore mittente invia il messaggio al gestore destinatario inserendolo in una busta di trasporto firmata per permettere al gestore destinatario di verificarne l'inalterabilità durante il trasporto. La busta, per definizione, contiene il messaggio e i suoi allegati, che quindi sono a loro volta protetti dalla firma del gestore. La Busta di Trasporto è il messaggio creato dal server smtps utilizzato dal mittente per l'invio: contiene il Messaggio originale inviato dall'utente e i dati di certificazione messi in allegato al messaggio generato come busta di trasporto. La busta di trasporto è firmata con la chiave del gestore di posta certificata mittente e viene recapitata nella casella di posta certificata del destinatario IMMODIFICATA per consentire la verifica dei dati di certificazione da parte del server ricevente.
- Il gestore destinatario, una volta ricevuto il messaggio PEC, consegnerà al gestore mittente una ricevuta di presa in carico che attesta il passaggio di consegne tra i due gestori. Il gestore destinatario verifica in fase di ricezione la correttezza del messaggio (anche riguardo all'integrità, grazie alla verifica della firma digitale) e si accerta che non siano presenti virus informatici.
- Nel caso il messaggio superi i suddetti controlli, viene consegnato alla casella di posta del destinatario che può quindi leggerne il contenuto.
- Al mittente perviene una ricevuta di avvenuta consegna, che attesta la disponibilità del messaggio presso il destinatario. La ricevuta è ancora una volta firmata digitalmente e attesta l'integrità del contenuto trasmesso (a meno di scegliere intenzionalmente una forma molto leggera di ricevuta).

È importante sottolineare che la posta elettronica certificata offre la garanzia della consegna del messaggio e non della sua lettura da parte del destinatario.

In altre parole nulla è detto sul fatto che il destinatario abbia letto o meno il messaggio PEC, ma si hanno garanzie sull'avvenuto recapito. Il che, in termini legali, equivale alla raccomandata con ricevuta di ritorno, ma con in più la prova certa del contenuto.

Questo e' possibile in quanto la posta certificata ha le seguenti caratteristiche:

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

La pec e le ricevute

Pertanto da quando detto finora si evince che per la certificazione del messaggio vengono emesse in particolare tre tipi di ricevute in caso di esito positivo per la consegna del messaggio:

- **Ricevuta di accettazione**, che attesta l'avvenuto invio della mail dal gestore di posta elettronica certificata del mittente.
- **Ricevuta di presa in carico**, che attesta il passaggio di responsabilità tra due distinti gestori di posta certificata, mittente e destinatario. Questa ricevuta viene scambiata tra i due gestori e non viene percepita dagli utilizzatori del servizio.
- **Ricevuta di avvenuta consegna**, che attesta che il messaggio è giunto a buon fine e che il destinatario ne ha piena disponibilità nella sua casella (anche se non ha ancora ricevuto il messaggio).

Dobbiamo precisare qualcosa in più per quanto riguarda le ricevute di avvenuta consegna in quanto a seconda delle esigenze specifiche infatti il Gestore può emettere tre differenti tipologie di Ricevute di Avvenuta Consegna, che possono soddisfare differenti esigenze dell'utenza:

- **la Ricevuta Completa** è costituita da un messaggio di posta elettronica inviato al mittente che riporta in formato leggibile i dati di certificazione (mittente, destinatario, oggetto, data e ora di avvenuta consegna, codice identificativo del messaggio). Gli stessi dati sono inseriti all'interno di un file XML allegato alla ricevuta. Per le consegne relative ai destinatari primari del messaggio (che sono i destinatari diretti del messaggio diversi dai destinatari riceventi in copia), la ricevuta di avvenuta consegna contiene anche il messaggio originale, testo ed eventuali allegati;

- **la Ricevuta Breve** ha lo scopo di ridurre i flussi di trasmissione della Posta Elettronica Certificata, soprattutto in quei casi in cui la mole di documenti e di messaggi scambiati è molto consistente. Per questo, la Ricevuta Breve contiene il messaggio originale e gli hash crittografici degli eventuali allegati. Per permettere la verifica dei contenuti trasmessi, il mittente deve conservare gli originali non modificati degli allegati inseriti nel messaggio originale a cui gli hash fanno riferimento;

- **la Ricevuta Sintetica** segue le regole di emissione della ricevuta completa solo che l'allegato contiene esclusivamente il file XML con i dati di certificazione descritti. La

ricevuta sintetica è particolarmente utile per i servizi che includono la Posta Elettronica Certificata come strumento di trasporto a supporto di una forte automazione dei flussi di comunicazione.

Ed in caso di problemi quali ricevute ci sono?

In caso di situazione negativa esistono inoltre tre tipi di avvisi rilasciati dal sistema PEC:

- **Di non accettazione** (per virus o utilizzo di un mittente falso o utilizzo di destinatari in copia nascosta, vietati dalla PEC, o altri problemi).
- **Di mancata consegna**, che sarà inviata al mittente entro 24 ore.
- **Di rilevazione di virus** informatici.

Nel caso in cui il messaggio sia inviato contemporaneamente a più destinatari di Posta Elettronica Certificata PEC, il mittente si vedrà recapitare una sola ricevuta di accettazione e tante ricevute di avvenuta consegna, o di non avvenuta consegna, una per ogni destinatario.

Se, invece, il messaggio è stato inviato a uno o più destinatari di posta ordinaria (non certificata), oltre a non avere alcun valore legale, non verranno generate le ricevute di avvenuta consegna.

Precisiamo anche che i messaggi in ingresso al sistema PEC possono essere "imbustati" dal gestore in due differenti tipologie di buste:

- **Di trasporto**, se il messaggio proviene da una casella di PEC e supera tutti i controlli di esistenza, provenienza e validità della firma.
- **Di anomalia**, se il messaggio proviene da una casella email non-PEC oppure è malformato, cioè non rispetta alcuni dei canoni per la creazione di un messaggio Pec.

Si aggiunge che i gestori e i domini da loro gestiti, in virtù del quadro normativo di riferimento, sono tutti censiti all'interno di una apposita struttura. Pertanto viene istituito un sistema di fiducia fondamentale per offrire all'utente tutte le garanzie di sicurezza caratteristiche di questo servizio.

Funzionamento del Servizio in caso di problemi di consegna

Possono verificarsi situazioni nelle quali il messaggio di Posta Elettronica Certificata non risulta consegnabile. In questo casi il funzionamento del sistema prevede che:

- se il gestore del mittente non riceve 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, allora il gestore del mittente stesso comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio.

- Se entro ulteriori dodici ore, il gestore del mittente non riceve 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.

Confidenzialità, Integrità e privacy della Posta elettronica Certificata

La traccia informatica delle operazioni svolte viene conservata per 30 mesi in un apposito registro informatico custodito dai gestori PEC, pertanto anche nel caso di un'accidentale o voluta perdita delle ricevute da parte del mittente o del destinatario, sarà comunque possibile risalire alle e-mail pec scambiate tramite tale registro, che garantisce al contempo il mittente ed il destinatario da eventuali problematiche e controversie.

Ad esempio il mittente non potrà negare di aver inviato una e-mail pec, di cui risulta traccia nel registro, ed un destinatario per lo stesso motivo non potrà negare di averla ricevuta.

La conservazione per 30 mesi delle ricevute include anche l'intero messaggio e suoi eventuali allegati che sono in chiaro cioè né più e né meno come quelli della normale raccomandata inseriti nella "busta di trasporto" "firmata digitalmente" almeno per tutto il periodo previsto.

contrariamente alla raccomandata che viene trattenuta dall'ufficio postale il tempo stabilito dal regolamento postale e poi restituita integra al mittente a compiuta giacenza, non è stabilito dalla normativa che fine faccia tutta la corrispondenza PEC dopo i trenta mesi.

È importante evidenziare che log dei messaggi non significa contenuto dei messaggi stessi, ma solo traccia dell'avvenuta transazione.

Secondo quanto previsto nelle regole tecniche allegate al DM 2 novembre 2005 i campi dovranno contenere almeno informazioni circa:

- Message-ID, codice identificativo del messaggio originale
- data dell'evento
- ora dell'evento
- mittente
- destinatario
- oggetto del messaggio
- tipo di evento (ad esempio ricevuta di accettazione o avvenuta consegna)
- Message-ID dei messaggi correlati
- gestore mittente

Il gestore PEC è l'unico ad avere le credenziali per aprire "la busta di trasporto" con tutto il suo contenuto. La capienza contrattualizzata delle caselle di posta impongono severi limiti alla libera circolazione della corrispondenza, nella normativa non esiste cenno a cosa accada se la serie di messaggi PEC supera la capienza della casella acquistata, sia dal mittente, sia dal ricevente. Tecnicamente, poiché la PEC si basa sulla tecnologia della posta elettronica, se la casella del destinatario è piena riceveremo - in luogo della ricevuta di avvenuta consegna - un messaggio di errore che ci informa, con la relativa diagnostica, dell'impossibilità di consegnare il messaggio.

È importante porre ora l’attenzione su come funziona la busta di trasporto, cioè il veicolo con cui i due provider di posta certificata comunicano e si trasferiscono le email certificate. La garanzia che la busta di trasporto sia inalterata durante il trasferimento da un gestore Pec all'altro è dovuta all’utilizzo dello standard S/MIME (*Secure/Multipurpose Internet Mail Extensions*).

Lo standard S/MIME si basa sull’utilizzo di certificati digitali che permettono di firmare e crittografare le e-mail, secondo algoritmi di criptografia asimmetrica.

Grazie all'utilizzo di tali certificati è possibile garantire l’integrità del messaggio semplicemente apponendo una firma digitale sul messaggio stesso.

Il provider del mittente crea la busta di trasporto, vi inserisce l’email del mittente e la firma digitale

grazie ad proprio certificato digitale. Il provider del destinatario, grazie a questa firma digitale, può verificare che la busta di trasporto sia integra e, quindi, accettarla o meno.

Tuttavia è importante sottolineare come la PEC non garantisca a priori l'integrità del messaggio.

La PEC, così strutturata, garantisce solamente che l'email inviata dal mittente non venga alterata durante il trasferimento da provider a provider, ma non garantisce che l'e-mail scritta dal mittente non sia stata alterata nel percorso tra il mittente e il provider del mittente.

Ed è per questo che entra in gioco l'utilizzo dei certificati S/MIME come strumento per garantire l'integrità dell'email inviata.

Qualsiasi utente può disporre di un proprio certificato digitale S/MIME, grazie al quale può firmare le proprie e-mail digitalmente. Firmando digitalmente la propria e-mail, questa e-mail assumerà valore legale in quanto si garantiscono le seguenti caratteristiche:

- **Confidenzialità**: segretezza dell'informazione scambiata.
- **Integrità**: garanzia che l'informazione non è stata alterata durante il trasporto.
- **Non ripudio**: certezza di possedere informazioni che provino l'origine (mittente) e la destinazione dei dati.

Cosa garantisce la Pec

- Il messaggio proviene da un gestore di posta certificato.
- Il messaggio non può essere alterato durante la trasmissione.
- Consente la privacy totale della comunicazione.
- Garantisce al mittente la certezza dell'avvenuto recapito delle e-mail.
- Garantisce in modo inequivocabile l'attestazione della data di consegna e di ricezione del messaggio.
- Garantisce il destinatario.

La normativa impone ai Gestori di PEC di applicare tutte le procedure atte a garantire la sicurezza e la privacy dei dati personali.

Pertanto si osserva che la responsabilità che grava sul gestore è elevata: un errore nell'identificazione di un soggetto, oppure una "falsa" ricevuta potrebbero cagionare danni gravissimi.

Per questo il soggetto gestore deve dimostrare una solidità finanziaria sufficiente a garantire la propria solvibilità in casi di questo genere. Difficilmente un piccolo operatore potrebbe essere affidabile per l'utenza, dato che potrebbe "sparire" dopo aver causato un danno. Sul fronte della concorrenza è da notare che nel Settembre 2009 l'elenco pubblico dei gestori di PEC operativi conta oltre 20 soggetti.

La Pec e i fornitori del servizio

I fornitori del servizio PEC prevedono sistemi di sicurezza aggiuntivi che garantiscano il servizio di Posta certificata e lo rendano affidabile.

Ad esempio aruba per fornire il servizio Pec garantisce i seguenti servizi di base:

- Presenza 3 livelli di firewalling con definizione di attente policy di accesso (vengono stabilite le sole porte strettamente necessarie al funzionamento del sistema PEC).
- Sistema di AntiVirus aggiornato con cadenza plurigiornaliera (almeno 4 volte al giorno) in modo da rendere il sistema protetto contro attacchi da parte di software malevolo.
- Prodotti software costantemente aggiornati e "patchati" (al rilascio di un nuovo prodotto o di una patch, dopo una fase di test su un ambiente di staging , viene aggiornato il prodotto in ambiente di produzione).
- Separazione fisica del livello di front end dal livello di back-end e storage in modo da proteggere ulteriormente in dati da accessi indesiderati.

Ulteriore protezione delle macchine che contengono i dati degli utenti attraverso firewall locali

- Sistema ridondato in ogni sua parte in modo da evitare "single point of failure".
- Meccanismo di auto esclusione degli apparati non funzionanti con conseguente dirottamento del traffico sugli altri nodi "gemelli"
- Utilizzo di storage di rete esterni al sistema per aumentare la protezione delle informazioni degli utenti.
- Sistema di backup su doppio supporto per ridurre il rischio di perdita dei dati.
- Utilizzo di protocolli sicuri per il colloquio tra l'utente ed il proprio gestore (SMTP/S,POP3/S,IMAP/S) e tra un gestore e l'altro (STARTTSL)
- Firma dei messaggi con i dispositivi HSM certificati FIPS-2 Level 3.

Vantaggi e Svantaggi

Il servizio PEC, per sua stessa natura, mostra una serie di vantaggi rispetto alla raccomandata con ricevuta di ritorno tradizionale. I principali sono:

- Ogni formato digitale può essere inviato tramite posta elettronica certificata;
- I messaggi possono essere consultati da ogni computer connesso a internet;
- Certificazione degli allegati al messaggio;
- L'avvenuta consegna della mail viene garantita, nel caso non sia possibile consegnare il messaggio l'utente viene informato;
- Le ricevute di consegna hanno validità legale;
- Tracciabilità della casella mittente e conseguentemente del suo titolare (se il titolare è stato identificato con certezza);
- Vi è certezza sulla destinazione dei messaggi;
- L'invio dei messaggi può avere costi inferiori a quello delle raccomandate. Per una giusta valutazione deve essere preso in considerazione il costo di invio di una raccomandata cartacea tradizionale, che cresce in funzione del numero di pagine e del peso del plico, e il numero di comunicazioni inviate annualmente. Queste informazioni devono poi essere comparate con le tariffe del gestore PEC, che solitamente rende disponibile una casella PEC con un costo calcolato su base annuale. Solitamente una volta pagato il canone annuale l'utente può inviare un numero illimitato di messaggi PEC. Va anche calcolato il total cost of ownership del servizio legato alle necessità di storage locale, backup, indicizzazione e retrieval delle ricevute, specie in grandi organizzazioni che generano rilevanti quantità di corrispondenza;
- Elevati requisiti di qualità e continuità del servizio. I Service Level Agreement (SLA) di legge prevedono una disponibilità del servizio del 99.8% su base quadrimestrale. Gli SLA della disponibilità del servizio PEC non valgono per la connettività. In altri termini, i server del gestore PEC possono essere disponibili nel 99,8% dell'anno, ma la connettività per raggiungerli (offerta da una terza parte) potrebbe avere SLA differenti;

- Obbligo da parte del gestore di archiviare tutti gli eventi associati ad invii e ricezioni di messaggi PEC, per un periodo di trenta mesi;
- Obbligo da parte del gestore di applicare le procedure atte a garantire il rispetto delle misure di sicurezza previste dal Codice dei dati personali e la sicurezza della comunicazione.

Al contempo vi sono alcuni svantaggi che possono portare a gravi difficoltà di interoperabilità:

- L'introduzione della Pec comporta una inevitabile perdita d'importanza della mail collegata al dominio aziendale.
- La Pec è un mezzo di comunicazione valido solo per l'italia, mandare una mail certificata all'estero è completamente inutile.
- Le mail certificate possono essere cancellate, si immagini quindi cosa accadrebbe se all'insaputa di un utente venisse rimosso dal suo computer un messaggio di cui non ha avuto notizia.
- La mail certificata inviata ad un destinatario certificato riceve una conferma di recapito, ma se il destinatario non possiede una casella certificata non avrà nessun valore legale.
- La mail certificata inviata ad una casella di posta comune non ottiene alcuna risposta "certa" di consegna.

La Cec Pac

Col l'avvento della Pec è nato un nuovo termine Cec Pac il cui acronimo significa **Comunicazione Elettronica Certificata tra la Pubblica Amministrazione e il Cittadino** ed è una modalità di posta certificata gratuita per il cittadino, che consente di dialogare esclusivamente con la pubblica amministrazione. Tale sistema di Posta Elettronica Certificata è riservata per lo scambio di messaggi con la pubblica amministrazione, e con tale modalità non è possibile effettuale alcuna comunicazione al di fuori.

Conclusioni

La PEC offre un servizio più completo e sicuro, prevedendo livelli minimi di qualità del servizio e di sicurezza stabiliti dalla legge ed una casella di PEC è indicata soprattutto per effettuare comunicazioni ufficiali per le quali il mittente vuole avere delle evidenze con valore legale dell'invio e della consegna del messaggio.

La PEC offre un servizio affidabile e garantito , infatti i gestori e i domini da loro gestiti, in virtù del quadro normativo di riferimento, sono tutti censiti all'interno di una apposita struttura. Pertanto viene istituito un sistema di fiducia fondamentale per offrire all'utente tutte le garanzie di sicurezza caratteristiche di questo servizio.

Per avere un'idea del volume di traffico, i numeri ufficiali relativi al primo bimestre dell'anno 2009 parlano di circa 300.000 caselle e di 30 milioni di messaggi.