PECI (POSTA ELETTRONICA CERTIFICATA A VALIDITÀ INTERNA) UNA OPPORTUNITÀ PER LA P.A.

Giovanni Battista Barone, Davide Bottalico, Ciro Di Mauro, Nicola Ranaldo, Amerigo Izzo
[giovannibattista.barone,davide.bottalico,ciro.dimauro,nicola.ranaldo,amerigo.izzo]@unina.it
Centro di Servizi Informativi di Ateneo (C.S.I.)
Università degli Studi di Napoli – Federico II

La Pubblica Amministrazione, attraverso l'introduzione e lo sviluppo di nuove tecnologie informatiche, ha una straordinaria opportunità di innovazione e miglioramento per l'erogazione di servizi ai cittadini e la possibilità di semplificare e rendere efficienti i servizi. In questa prospettiva, lo studio e la sperimentazione della Posta Elettronica Certificata rappresenta uno strumento innovativo per la linearizzazione e la semplificazione dei suoi processi. Il decreto del Presidente della Repubblica recante regolamento concernente disposizioni per l'utilizzo della posta elettronica certificata, approvato dal consiglio dei ministri del 28 gennaio 2005, ha aperto un nuovo scenario per la comunicazione tra cittadino e Pubblica Amministrazione. In quest'articolo si vuole dare uno spunto di riflessione alle opportunità offerte dalla Posta Elettronica Certificata (PEC) alle Pubbliche Amministrazioni, come l'università, che hanno un vastissima utenza ma ben definita. L'idea di base non è quella di proporre alle università di diventare fornitori di posta certificata ma di utilizzare tutta la tecnologia e gli studi effettuati in materia per creare un canale di comunicazione unico certo ed affidabile tra università/studenti e università/dipendenti, in altre parole creare un sistema di posta elettronica certificata a validità interna.

1. PEC Il punto di arrivo legislativo

Il decreto del presidente della repubblica recante regolamento concernente disposizioni per l'utilizzo della posta elettronica certificata, approvato dal consiglio dei ministri del 28 gennaio 2005, è solo l'ultimo atto di un percorso legislativo iniziato con il Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 che afferma "...Le pubbliche amministrazioni provvedono entro il 1° gennaio 2004 a realizzare o revisionare sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi in conformità alle disposizioni del presente testo unico.."e con l'Art. 14 punto 3. "La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge". Questo percorso conduce alla definizione delle regole tecniche di quello che si può definire l'equivalente telematico della raccomandata con ricevuta di ritorno. Infatti, quello che è certificato non è il contenuto ma il processo che porta la consegna del documento.[1]

1.1. Commento legislativo

Non riportiamo il decreto ma per chiarezza portiamo alcuni commenti esplicativi del suo significato cercando di fugare i dubbi e le incomprensioni in cui si può incappare in una sua lettura superficiale.

La firma digitale sulla busta non ha nulla a che fare con l'eventuale firma digitale sul documento trasmesso:
Si possono trasmettere con la PEC sia documenti firmati digitalmente sia documenti non firmati.
I documenti non firmati non possono acquistare il valore di documenti firmati solo per il fatto che sono trasmessi attraverso la posta certificata
La firma del gestore non dice nulla circa l'effettiva identità del mittente e l'origine del documento.
La ricevuta di consegna attesta solo che il messaggio è stato recapitato nella casella del destinatario, non che lo abbia scaricato o letto.
Si presume, salvo prova contraria, che il ricevente abbia letto il documento, esattamente come per la raccomandata postale
L'avviso di ricevimento non dice nulla sull'effettiva apertura del plico o della busta e sulla lettura del contenuto.

1.2. Le regole tecniche

Un approfondito studio, ed una sperimentazione ad ampio spettro, sono stati condotti prima di giungere a quelle che vengono definite le regole tecniche. Un gran plauso deve essere fatto a chi ha collaborato ed ha portato l'Italia all'avanguardia in questo settore. Infatti, molti sono i paesi che attendono l'introduzione della PEC in Italia per far tesoro della nostra esperienza ed applicarla nel loro contesto legislativo. Il risultato delle regole tecniche sono una sequenza semplice ma rigorosa di definizioni dei punti salienti che sono coinvolti nel processo. Di seguito riportiamo le definizioni dei punti essenziali.
Punto di accesso È il punto che fornisce i servizi di accesso per l'invio di messaggi di posta certificata. Il punto di accesso fornisce i servizi di accesso dell'utente, emissione della ricevuta di accettazione, imbustamento del messaggio originale nel messaggio di trasporto.
Punto di ricezione È l'entità che riceve il messaggio all'interno di un dominio di posta certificata. Corrisponde alla macchina destinata alla ricezione dei messaggi per il dominio. Effettua i controlli sulla provenienza/correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in un messaggio di anomalia di trasporto.
Punto di consegna Effettua la consegna del messaggio nella casella di posta elettronica dell'utente di posta certificata destinatario. Verifica la provenienza/correttezza del messaggio, emette la ricevuta di avvenuta consegna.
Ricevuta di accettazione È la ricevuta, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta certificata. La ricevuta di accettazione è firmata con la chiave del gestore di posta certificata del mittente. (Figura1)

Ricevuta di presa in carico È emessa dal punto di ricezione verso il gestore di posta certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del dominio di posta certificata di destinazione. Nella ricevuta di presa in carico sono inseriti i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce.
Ricevuta di avvenuta consegna Il punto di consegna emette al mittente la ricevuta di avvenuta consegna nel momento in cui il messaggio è inserito nella casella di posta certificata del destinatario. È rilasciata una ricevuta di avvenuta consegna per ogni destinatario al quale il messaggio è consegnato. La ricevuta di avvenuta consegna porta in allegato i dati di certificazione e, per i destinatari primari del messaggio, il messaggio originale.(figura2)

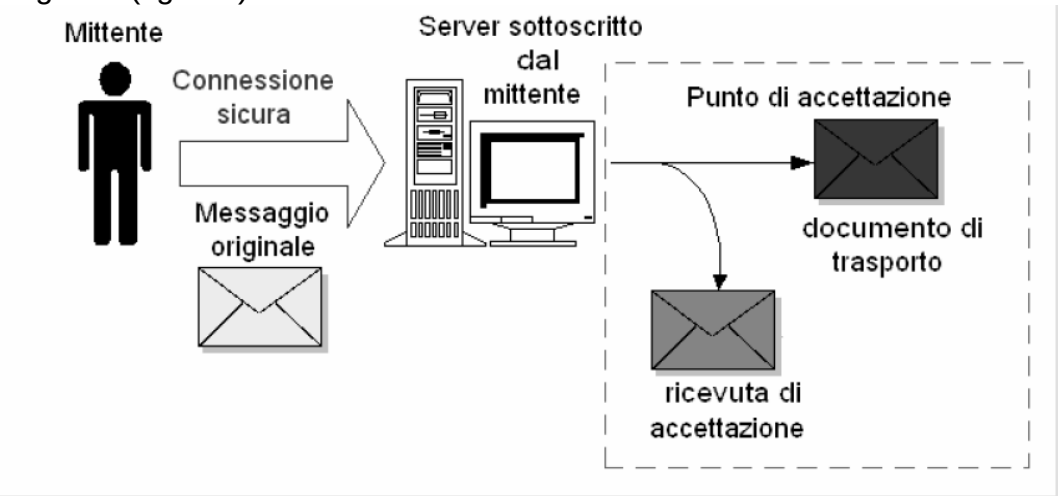

Figura 1

Ricevuta di errore di consegna Nel caso in cui il punto di consegna sia impossibilitato a consegnare il messaggio nella casella di posta certificata del destinatario, il sistema emette una ricevuta di errore di consegna per indicare l'anomalia al mittente del messaggio originale.
Messaggio originale È il messaggio originale inviato da un utente di posta certificata prima del suo arrivo al punto di accesso. Il messaggio originale è consegnato all'utente di posta certificata di destinazione per mezzo di un messaggio di trasporto che lo contiene.
Messaggio di trasporto È il messaggio creato dal punto di accesso, all'interno del quale è inserito il messaggio originale inviato dall'utente di posta certificata ed i relativi dati di certificazione. Il messaggio di trasporto è firmato con la chiave del gestore di posta certificata mittente. Il messaggio di trasporto è consegnato immodificato nella casella di posta certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente.
Messaggio di anomalia di trasporto Quando un messaggio errato/non di posta certificata deve essere consegnato ad un utente di posta certificata, il messaggio è inserito in un messaggio di anomalia di trasporto per evidenziare l'anomalia al destinatario. Il messaggio di anomalia di trasporto è firmato con la chiave del gestore di posta certificata del destinatario.

Dati di certificazione Sono un insieme di dati che descrivono il messaggio originale e sono certificati dal gestore di posta certificata del mittente. I dati di certificazione sono inseriti nelle varie ricevute e sono trasferiti all'utente di posta certificata di destinazione insieme al messaggio originale per mezzo di un messaggio di trasporto. Tra i dati di certificazione sono: data ed ora di invio, mittente, destinatario, oggetto, identificativo messaggio, ecc.

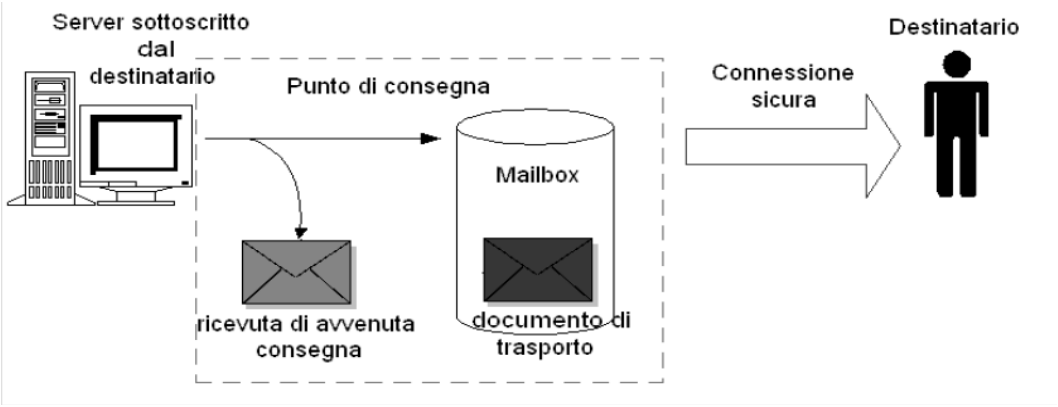

Figura 2

Gestore di posta certificata È un entità che gestisce uno o più domini di posta certificata con i relativi punti di accesso, ricezione e consegna. È titolare della chiave usata per la firma delle ricevute e dei messaggi di trasporto. Si interfaccia con altri gestori di posta certificata per l'interoperabilità con altri utenti di posta certificata. (Figura3)

Dominio di posta certificata Corrisponde ad un dominio DNS dedicato alle caselle di posta elettronica degli utenti di posta certificata. All'interno di un dominio di posta certificata tutte le caselle di posta elettronica devono appartenere ad utenti di posta certificata.

Indice dei gestori di posta certificata Consiste in un server LDAP posizionato in un'area raggiungibile dai vari gestori di posta certificata. Contiene l'elenco dei domini e dei gestori di posta certificata con i relativi certificati relativi alle chiavi usate per la firma delle ricevute e dei messaggi di trasporto.

Casella di posta certificata È una casella di posta elettronica alla quale è associata una funzione che rilascia delle ricevute di avvenuta consegna al ricevimento di messaggi di posta certificata.

Utente di posta certificata È un utente a cui è assegnata una casella di posta certificata. Utilizza il punto di accesso del proprio gestore di posta certificata per inviare messaggi di posta certificata.

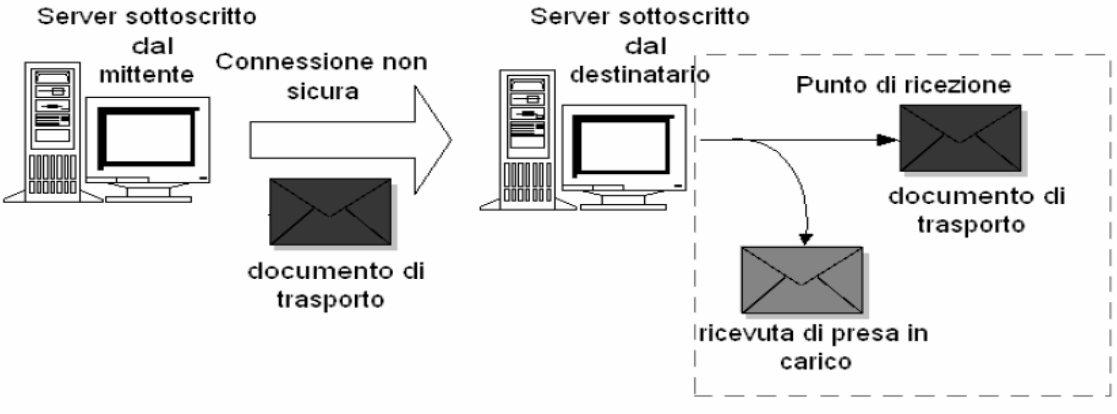

Figura 3

1.3. Riferimento temporale

Elemento importante e decisivo per la verifica delle avvenute transazioni è il riferimento temporale. Ancora una volta c'è da fare un plauso al legislatore che ha reso questo elemento meno rigido conservando la rigorosità necessaria del riferimento

Per tutte le operazioni effettuate durante i processi di elaborazione dei messaggi, ricevute, log, ecc. svolte dai punti di accesso/ricezione/consegna è necessario disporre di un accurato riferimento temporale. Tutti gli eventi (generazione di ricevute, messaggi di trasporto, log, ecc.) che costituiscono la transazione di elaborazione del messaggio presso i punti di accesso, ricezione e consegna devono impiegare un unico valore temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, ricevute, messaggi, ecc. generati dal server. **Il riferimento temporale può essere generato con qualsiasi sistema che garantisca uno scarto non superiore ad 1 secondo rispetto al Tempo Universale Coordinato (UTC).**

2. L'OpenPEC

OpenPEC è un progetto Open Source nato per rendere un sistema di posta elettronica convenzionale, un sistema Certificato secondo le linee guida emesse dal CNIPA. E' sviluppato interamente in Perl e progettato in modo da essere modulare e scalabile (integrato con OpenCA)[2].

L'implementazione si basa su Amavis (branch amavis-new) dal quale eredita la compatibilità con i più diffusi mail server. (Si può affermare, senza ombra di smentita, che ancora una volta le idee semplici ma concrete, consentono la risoluzione di problemi complessi. (figura4)

2.1. Caratteristiche

OpenPEC può essere visto come un "plug-in" di sistemi di posta esistenti ha la compatibilità con i più diffusi MTA (Mail Transfer Agent) possiede una interfaccia modulare ed attualmente vengono gestiti i protocolli ESMTP e LMTP

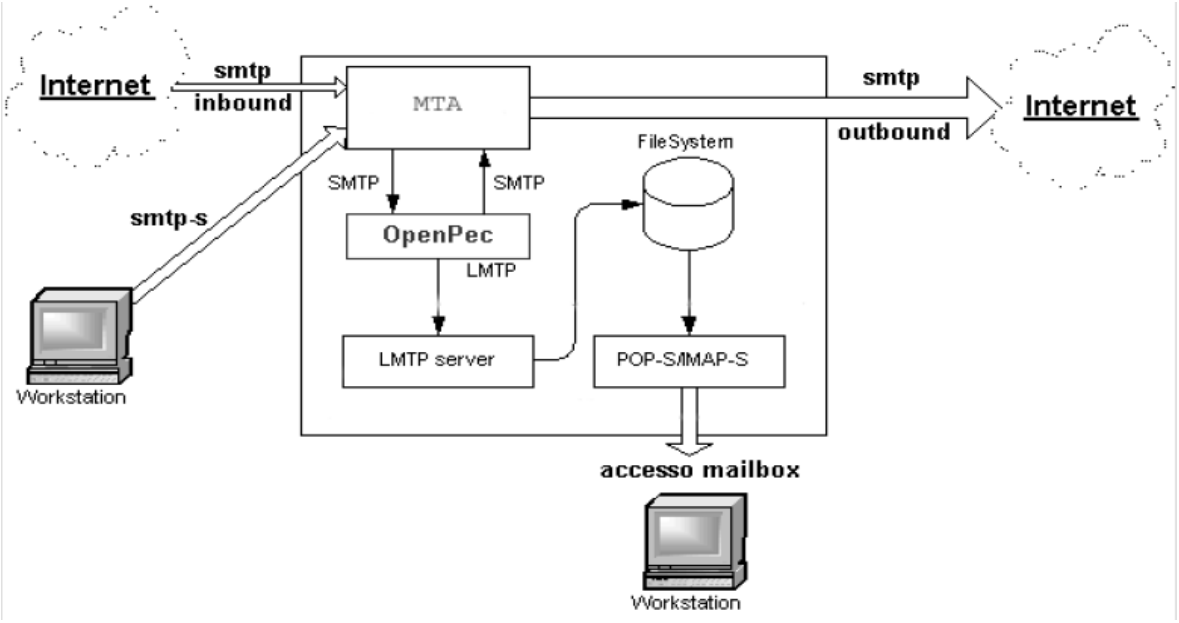

Figura 4

2.2. Affidabilità

In un sistema così critico l'elemento chiave è l'affidabilità più che dal punto di vista HW dal punto di vista del software utilizzato. OpenPec in tal senso ha degli elementi chiave che consentono un ottimo grado di affidabilità dell'intero processo e cioè:
La mail viene salvata su file durante la ricezione
OpenPEC non è mai direttamente responsabile della mail
Sistema di Fault Recovery: in caso di errori la mail viene mantenuta nella coda del MTA e rielaborata successivamente

2.3. Certificati Necessari

I certificati necessari all'implementazione di qualsiasi sistema di PEC sono gli elementi che maggiormente portano a confusione su quello che è lo scopo di PEC e cioè un sistema di "raccomandata Telematica". I certificati digitali sono necessari proprio per certificare i vari passaggi e fasi del processo di una PEC. Sono necessari 2 tipi di certificati (figura5):
1 o più certificati per le connessioni TLS IMAPS POPS SMTPS HTTPS;
Un certificato x509 (S/MIME) per la firma delle mail in uscita.

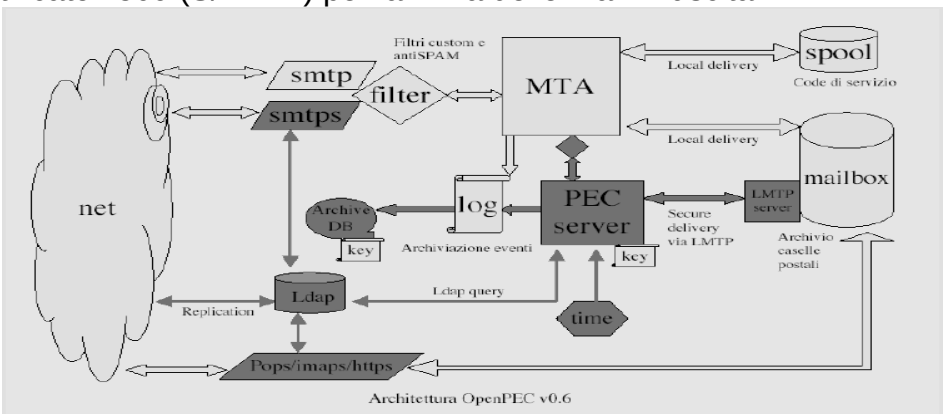

Figura 5

E’ bene ricordare, che il nostro scopo consta nel realizzare un canale di comunicazione, sicuro e certo, con la platea dei possibili fruitori dei servizi dell’università. A tal scopo possono essere utilizzati, serenamente, certificati ottenuti con sì un sistema di PKI rigoroso, ma sicuramente a validità interna (OpenCA).

2.4. Possibilità per le P.A.

L’utilizzo delle regole tecniche consente al processo anche se a validità interna di avere gli stessi crismi di un sistema ufficiale di PEC mettendo al sicuro da brutte sorprese le PA che lo volessero utilizzare come canale di comunicazione. Il progetto consiste nel realizzare un sistema PEC a validità interna per attuare un canale sicuro ed affidabile di comunicazione tra studente e università e tra dipendente ed università.
Attraverso questo sistema, infatti, le segreterie possono comunicare avvisi allo studente o inviare modifiche della data di esame o lo studente stesso trasmettere richieste ufficiali o iscrizione verso la segreteria. Per la comunicazione tra università e dipendente l’applicazione immediata sta nella trasmissione del cedolino paga, nella trasmissione del cud. Come si vede l’introduzione di uno strumento affidabile e sicuro consente di veicolare tutti i processi che richiedono una comunicazione cartacea del tipo raccomandata con ricevuta di ritorno consentendo in tal modo uno snellimento dei processi ed una accelerazione facendo crescere sia l’efficienza che l’efficacia della P.A..
Riportiamo di seguito l’articolo 16 che nulla aggiunge ad una PEC con validità creata da una PA ad una PECI/PA a validità interna. Le pubbliche amministrazioni, infatti, che volessero certificarsi potranno fornire caselle di posta PEC solo per il trattamento delle comunicazioni che rientrano nella propria missione (studenti e o dipendenti e solo per comunicare con quella PA).
ART. 16 (Disposizioni per le pubbliche amministrazioni)
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.

3. Il Prototipo

Per l’attuazione del progetto è stato realizzato un prototipo di PECI (Posta Elettronica Certificata Interna) sfruttando la PKI a validità interna, realizzata da qualche tempo con OpenCA, utilizzando la nuova versione del prodotto OpenPEC (OpenPec2) completamente aderente alla normativa vigente, resa compatibile per l’ambiente operativo Linux Gentoo attraverso opportune operazioni di porting (non essendo stato sviluppato per tale Sistema Operativo) ed utilizzando come sistema di posta la terna affidabile e consolidata postfix sasl cyrus.
L’accesso al servizio di posta elettronica certificata interna (PECI), può avvenire attraverso i più comuni MUA (Mail User Agent) Outlook Express,
Eudora, Mozilla Thunderbird ecc, oppure tramite webmail realizzata con il Frame Work Horde utilizzando un qualunque browser (Internet Explorer, Mozilla Firefox ecc).

Il prototipo cosi realizzato è stato sperimentato per la comunicazione delle matricole per un gruppo di studenti (circa 4000) attraverso la posta certificata di ateneo Federico II di Napoli, per testarne robustezza affidabilità e performance.
Infatti, grazie all'utilizzo anche del contact center di ateneo e alla sensibilizzazione delle segreterie studenti si è riusciti a raggiungere il 99% degli studenti (quando ci sono problematiche di carattere anagrafico l'email non viene creata automaticamente). Il servizio è stato accettato con piacere dalla platea studentesca soprattutto per la facilità d'uso e la certezza della notifica.
L'autenticazione degli studenti avviene in maniera centralizzata attraverso il directory di ateneo anch'esso realizzato con Openldap.
Sono state altresì effettuate prove di compatibilità che hanno dato ottimi risultati.

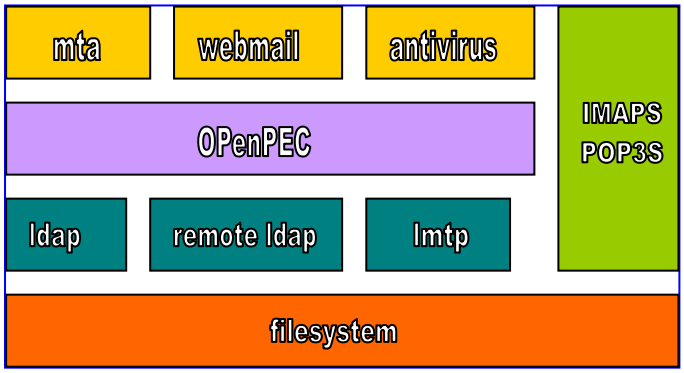

Figura 6

Come si può notare dallo schema (figura 6), il sistema di posta PECI ruota intorno ad OpenPEC che rappresenta il modulo centrale dell'intera architettura, e che a sua volta si interfaccia con tutti gli altri moduli del sistema e precisamente con:

1. L' MTA che si incarica del dispatching della mail,
2. il modulo antivirus che controlla qualsiasi messaggio sia ingresso che in uscita,
3. la webmail attraverso la quale l'utente può accedere al servizio di posta tramite web browser,
4. il server IMAPS/POP3S attraverso la quale l'utente accede alla propria mailbox,
5. il directory LDAP locale che contiene l'indice dei gestori pec,
6. il directory LDAP remoto che contiene tutte le informazioni necessarie per l'autenticazione degli utenti del sistema peci (directory di autenticazione centralizzato,
7. il modulo LMTP per il delivery dei messaggi nella mailbox degli utenti,
8. il filesystem che contiene tutti dati del sistema nonchè le mailbox degli utenti ed i file di log.

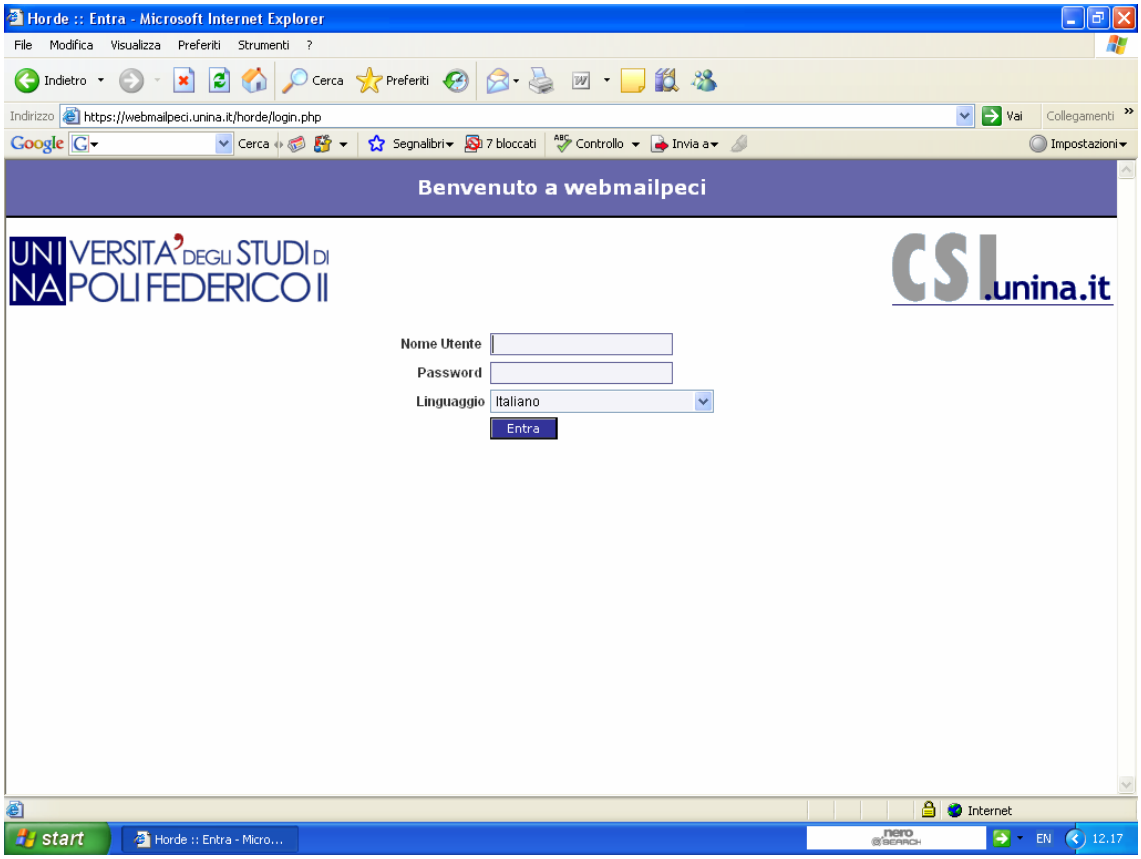

Figura 7

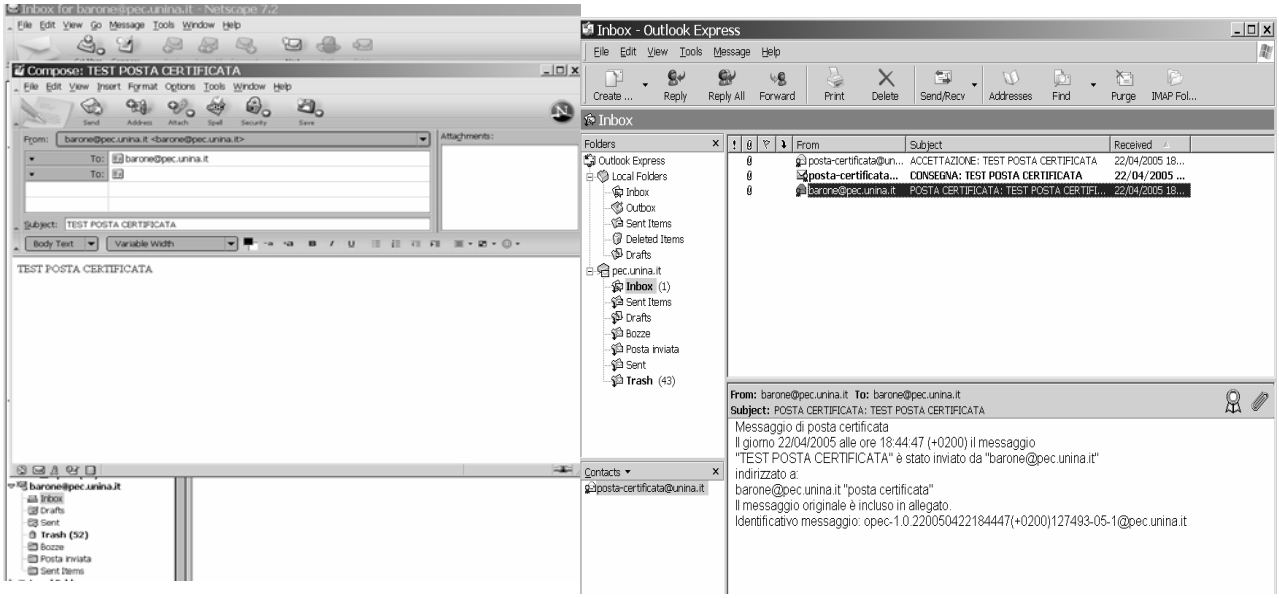

Figura 8

4. Sviluppi e lavori Futuri

La realizzazione e la progettazione del sistema ha beneficiato di tutto il lavoro sin ora sviluppato da CNIPA, dimostrando ancora una volta che

l’organizzazione e gli sforzi della PA portano sempre ad ottimi risultati che possono rappresentare il punto di riferimento per tutte le P.A.. La messa in produzione del sistema può essere realizzata solo a valle di un grande coinvolgimento del management della P.A. realizzato attraverso lo schema fornito dal Dizionario delle Forniture ICT, altro elemento fornito dal CNIPA.
Gli ottimi risultati della sperimentazione hanno dimostrato che il sistema è maturo per essere messo in produzione per la comunicazione istituzionale. Infatti, la prosecuzione del progetto prevede una separazione dell’email tra canale istituzionale per cui sarà utilizzata la PECI e una email open per tutto l’altro tipo di messaggi.
L’ultima fase del progetto consiste nella realizzazione di un pacchetto anche per il dipendente comprendente una email PECI all’atto della assunzione. Per rendere il servizio ancora più completo è in corso di realizzazione una procedura che consenta la lettura della Carta d’Identità Elettronica e l’utilizzo del certificato al suo interno per rendere sicuro anche il contenuto dell’email ottenendo in tal modo la posta certificata con certificazione di trasmissione/ricezione.

5. Riferimenti bibliografici

[1] http://www.cnipa.gov.it/site/it-IT/In_primo_piano/Posta_Elettronica_Certificata__(PEC)/

[2] http://sourceforge.net/projects/openpec2/

[3] http://www.openca.org/