


OpenPEC: La soluzione open source per la Posta Elettronica Certificata

Descrizione della soluzione

Autore	EXEntrica srl
Versione	1.0
Data	25. Sep. 2006

Indice

Glossario.....	3
La posta elettronica certificata (PEC).....	3
Riferimenti di legge.....	4
Come funziona un sistema di PEC.....	5
I gestori di PEC.....	6
Che cosa cambia per l'utente finale.....	6
OpenPEC.....	6
Architettura della soluzione.....	7
Prodotti utilizzati.....	10

	<i>OpenPEC: La soluzione open source per la Posta Elettronica Certificata</i>
	<i>OpenPEC-descrizione-sito</i>

Glossario


<i>Open Source</i>	In informatica, Open Source indica un software rilasciato con un tipo di licenza per la quale il codice sorgente è lasciato alla disponibilità di eventuali sviluppatori, in modo che con la collaborazione (in genere libera e spontanea) il prodotto finale possa raggiungere una complessità maggiore di quanto potrebbe ottenere un singolo gruppo di programmazione.
<i>MTA</i>	Mail Transfer Agent. E' un modulo che ha il compito di effettuare il dispatching dei messaggi di posta elettronica (invio e ricezione)
<i>LDAP</i>	<i>Lightweight Directory Access Protocol</i> . E' un protocollo di rete utilizzato per la ricerca e memorizzazione di informazioni su un Directory Server. Una directory server LDAP è un albero di entità costituite da attributi e valori. Un classico utilizzo di un directory server è la memorizzazioni degli account email o degli utenti registrati ad un sito.
<i>SMTP</i>	<i>Simple Mail Transfer Protocol</i> . Protocollo Standard per la trasmissione di email su internet
<i>SMTP/S</i>	SMTP con autenticazione sicura
<i>POP</i>	<i>Post Office Protocol</i> . Protocollo per l'accesso ad un account di posta elettronica
<i>POP/S</i>	POP con autenticazione sicura
<i>IMAP</i>	<i>Internet Message Access Protocol</i> . Protocollo per l'accesso ad un account di posta elettronica e per la lettura delle email.
<i>IMAP/S</i>	IMAP con autenticazione sicura
<i>LMTP</i>	<i>Local Mail Transfer Protocol</i> . Derivato dall'SMTP, lo può sostituire nei casi in cui il ricevente non gestisce la coda dei messaggi.
<i>HSM</i>	<i>Hardware Security Module</i> . Dispositivi hardware utilizzati per la firma delle mail.

La posta elettronica certificata (PEC)

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale al mittente viene fornita documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

La PEC è nata con l'obiettivo di trasferire su digitale il concetto di *Raccomandata con Ricevuta di Ritorno*. Come mezzo di trasporto si è scelto di utilizzare l'email che garantisce, oltre alla facilità di utilizzo e alla diffusione capillare sul territorio, una velocità di consegna non paragonabile alla posta tradizionale.

25. Sep. 2006	Copyright © 2006 EXEntrica srl Tutti i diritti riservati	Pagina 3 di 10
---------------	---	----------------

	<i>OpenPEC: La soluzione open source per la Posta Elettronica Certificata</i>
	<i>OpenPEC-descrizione-sito</i>

Attraverso la PEC chi invia una email ha la certezza dell'avvenuta (o mancata) consegna del proprio messaggio e dell'eventuale documentazione allegata.

Per certificare l'avvenuta consegna vengono utilizzate delle ricevute che costituiscono prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Le operazioni sono inoltre siglate con riferimenti temporali che "timbrano" in modo inequivocabile gli istanti di invio e ricezione.

Come garanti del servizio vengono costituiti dei **gestori certificati** da parte del Centro Nazionale Informatica per la Pubblica Amministrazione (CNIPA). I gestori possono essere sia Enti Pubblici che soggetti privati.

Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte viene conservata per un periodo di tempo definito a cura dei gestori, con lo stesso valore giuridico delle ricevute di risposta.

I messaggi possono includere testo, immagini, audio, video o qualsiasi altro tipo di file.

Riferimenti di legge

Il Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 [1] ha stabilito che a partire dal 2004 tutte le Pubbliche Amministrazioni (PA) (compresi Enti Locali, Istituti scolastici e universitari, etc) debbano adeguare i propri sistemi informativi per gestire lo scambio di documenti informatici tramite questo strumento.

Il DPR (Decreto del Presidente della Repubblica) del 11 febbraio 2005 [2] emana il regolamento che stabilisce le caratteristiche e le modalità per l'erogazione e la fruizione di servizi di trasmissione di documenti informatici mediante posta elettronica certificata.

Il 12 maggio 2005 il CNIPA emette le "Regole Tecniche del servizio di trasmissione dei documenti informatici tramite Posta Elettronica Certificata" [3] che definisce i requisiti tecnico-funzionali necessari per l'erogazione del servizio.

Il 16 giugno 2005 il CNIPA emette lo schema di DPCM (Decreto del Presidente del Consiglio dei Ministri) [4] che contiene l'elenco dei principi generali del sistema di PEC e delle disposizioni per i gestori di servizio. Rappresenta il documento di riferimento dei requisiti tecnico-funzionali e della documentazione necessaria.

Il 15 novembre 2005 viene pubblicato in Gazzetta Ufficiale il DPCM: da questo momento esiste la normativa legale ufficiale che regola la PEC.

Il 5 dicembre 2005 viene pubblicato in Gazzetta Ufficiale la Circolare CNIPA recante le modalità di presentazione della domanda di accreditamento nell'elenco pubblico dei Gestori di PEC [5].

25. Sep. 2006	Copyright © 2006 EXEntrica srl Tutti i diritti riservati	Pagina 4 di 10
---------------	---	----------------

A partire da questa data i soggetti pubblici e privati possono richiedere di certificarsi quali fornitori del servizio di PEC.

Come funziona un sistema di PEC

Il funzionamento di un sistema di Posta Elettronica Certificata può essere descritto sulla base del seguente schema. Per prima cosa è necessario dire che i messaggi di posta certificata vengono spediti tra 2 caselle, e quindi domini, certificati.

Nel disegno (Fig. 1) sono rappresentati 2 diversi domini di posta certificata e vengono evidenziati in rosso i percorsi del messaggio dal mittente al destinatario ed in azzurro i percorsi della ricevuta.

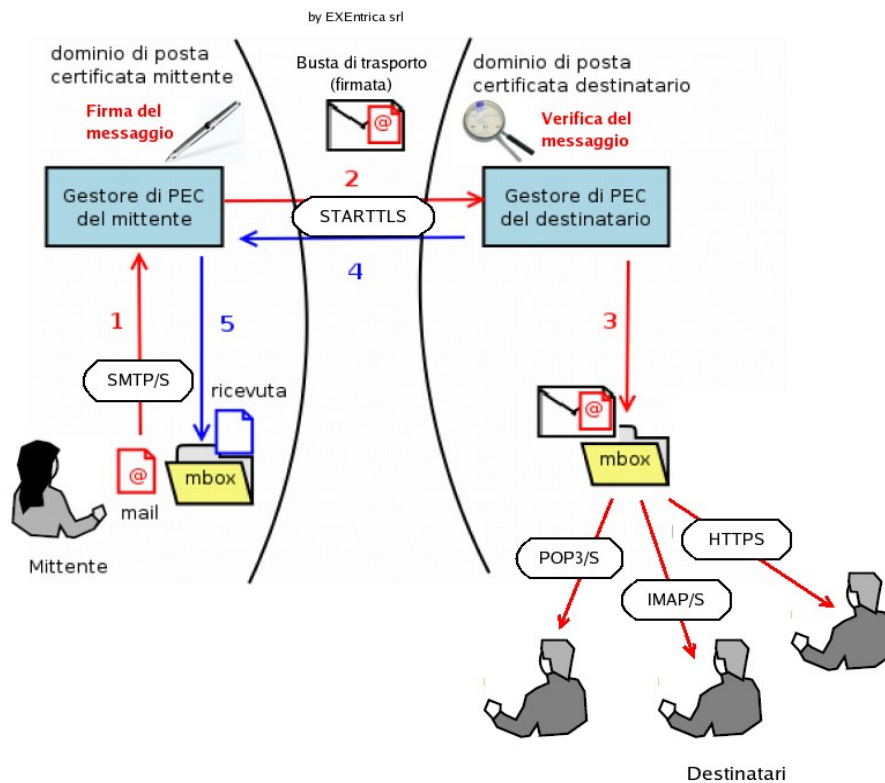


Fig.1- Funzionamento di un sistema di PEC



Nel dettaglio:

Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato (passo 1), il messaggio viene raccolto dal gestore del dominio certificato che lo racchiude in una busta di trasporto e vi applica una firma elettronica in modo da garantire inalterabilità e provenienza. Fatto questo indirizza il messaggio al gestore di PEC destinatario (passo 2) che verifica la firma e lo consegna al destinatario (passo 3).

Una volta consegnato il messaggio il gestore PEC destinatario invia una ricevuta di avvenuta consegna all'utente mittente (passi 4 e 5) che può essere quindi certo che il suo messaggio è giunto a destinazione.

I gestori di PEC

Come accennato in precedenza per il funzionamento della posta elettronica certificata, è fondamentale il ruolo dei gestori accreditati di PEC.

Per diventare gestore di PEC l'Ente Pubblico o il soggetto privato devono soddisfare una serie di requisiti (alcuni dei quali di natura economica per i privati) e devono seguire un percorso di acquisizione della certifica che parte dalla descrizione della propria architettura hardware, di rete e di sicurezza, fino alla esecuzione dei test di interoperabilità e gestione delle visite ispettive da parte dell'ente certificatore (CNIPA).


Una volta ottenuta la certifica, il gestore ha la facoltà applicare il proprio modello di business ad esempio vendendo le mailbox, facendo pagare il servizio di invio, ecc.

Che cosa cambia per l'utente finale

Per l'utente finale non cambia assolutamente niente in quanto può utilizzare la casella di PEC come una normale casella di posta. Sono sufficienti delle banali configurazioni per aggiungere l'account di posta certificata ai principali client sul mercato (Outlook, Outlook Express, Thunderbird, Eudora, etc.).

OpenPEC

OpenPEC è un progetto Open Source nato per realizzare un sistema di Posta Elettronica Certificata conforme alle linee guida indicate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).

	<i>OpenPEC: La soluzione open source per la Posta Elettronica Certificata</i>
	<i>OpenPEC-descrizione-sito</i>

OpenPEC non è un sistema di posta elettronica sviluppato completamente da zero ma si propone come estensione dei mail server Open Source più diffusi sul mercato, come Postfix, Sendmail e gmail, e, in prospettiva, dei sistemi commerciali. In quest'ottica, OpenPEC può essere visto come un "plug-in" di questi sistemi.

Secondo modalità specifiche legate all'implementazione dei singoli server, OpenPEC può anche essere "aggiunto" ad un sistema già installato e funzionante: in questo modo si garantisce una naturale evoluzione dei sistemi esistenti evitando difficili e spesso costose operazioni di migrazione o di conversione. Questa è sicuramente una caratteristica molto importante per chiunque debba adottare un sistema di PEC per lo scambio dei documenti.

OpenPEC è rilasciato con licenza Gnu GPL (General Public License).

La versione 2.0 del prodotto è completamente aderente alla normativa vigente.


Caratteristiche principali

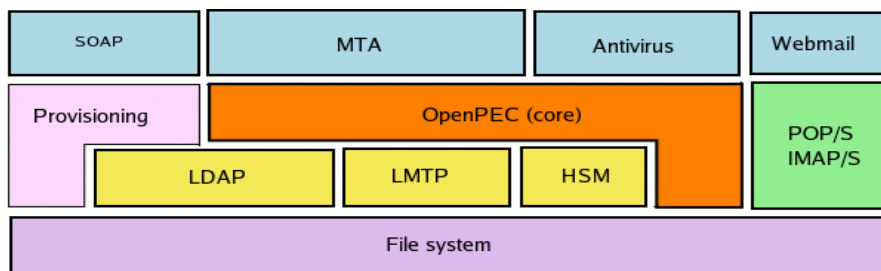
- *Piena compatibilità con la normativa vigente*
- *Prestazioni elevate*
- *Affidabilità*
- *Scalabilità*
- *Modularità*
- *Compatibilità con i principali fornitori di Hardware Security Module (HSM)*
- *Capacità di gestire sistemi con un elevato numero di domini e/o mailbox*
- *Aggiornamento automatico e trasparente dei domini locali (senza riavvio)*
- *Marcatura temporale e storicizzazione dei log*
- *Gestione delle Certificate Revocation List (CRL)*

Architettura della soluzione

Di seguito riportiamo uno schema (Fig. 2) che descrive i principali componenti di una soluzione di posta elettronica certificata basata su OpenPEC:

25. Sep. 2006	Copyright © 2006 EXEntrica srl Tutti i diritti riservati	Pagina 7 di 10
---------------	---	----------------

	<i>OpenPEC: La soluzione open source per la Posta Elettronica Certificata</i>
	<i>OpenPEC-descrizione-sito</i>



by EXEntrica srl

Fig. 2 - Componenti del sistema

Come è possibile vedere dallo schema, il **OpenPEC** rappresenta il nucleo centrale del sistema e si interfaccia con gli altri moduli:

- il Mail Transfer Agent (**MTA**) che si incarica del "dispatching" delle mail,
- il modulo **Antivirus** che controlla ogni messaggio che arriva,
- il server **LDAP** che contiene il mirror dell'indice dei gestori,
- il database (**RDBMS**) che contiene gli account di PEC,
- il server **LMTP** che si incarica di effettuare il delivery dei messaggi nelle mailbox degli utenti,
- i moduli **HSM** utilizzati per la firma dei messaggi (e per la verifica dei messaggi firmati),
- lo **storage** (file system) che contiene i dati del sistema fra cui le mailbox ed i file di log,
- i server **POP-IMAP** attraverso i quali l'utente ha la possibilità di accedere alla propria mailbox attraverso i comuni clienti di posta.
- la **web mail** attraverso la quale l'utente può accedere alla propria casella attraverso un comune internet browser,
- il modulo di **provisioning** (per la creazione/modifica degli account) richiamabile attraverso interfaccia SOAP

Per descrivere a grandi linee il funzionamento del sistema utilizziamo la Fig. 3 seguente nella quale sono evidenziate le interazioni tra i principali componenti.

25. Sep. 2006	Copyright © 2006 EXEntrica srl Tutti i diritti riservati	Pagina 8 di 10
---------------	---	----------------

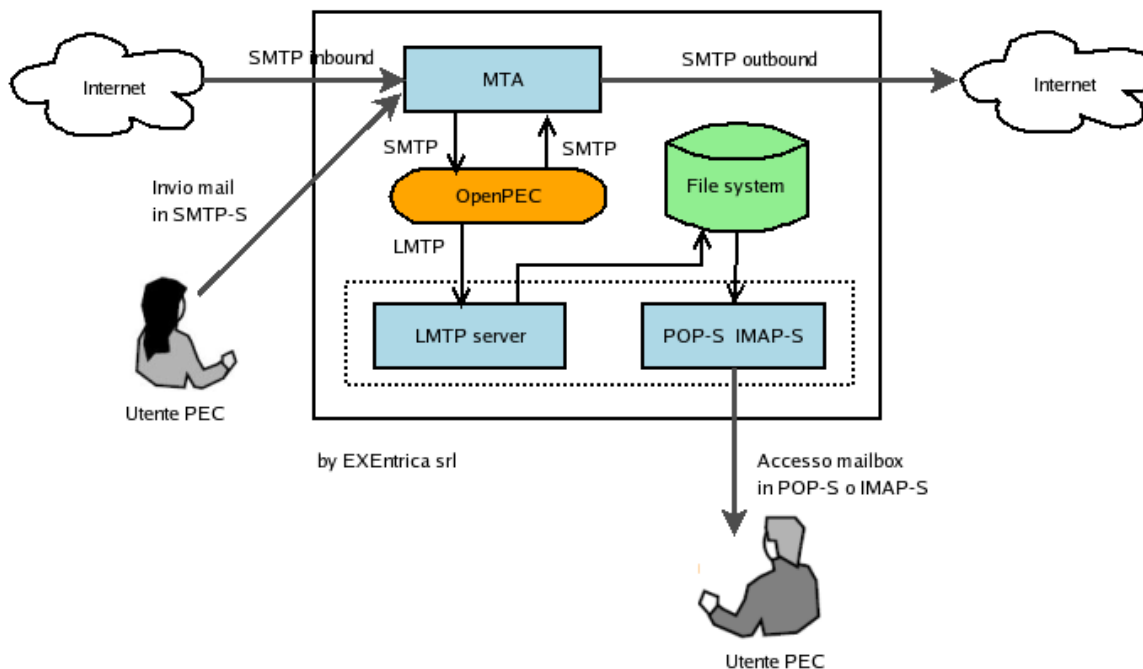



Fig. 3 – Interazioni tra i moduli del sistema

Per ogni messaggio che arriva ad OpenPEC dall'MTA:

- se è un **messaggio in uscita** lo incapsula in un documento di trasporto, lo firma elettronicamente attraverso il modulo HSM e lo restituisce all'MTA che lo inoltra verso il destinatario;
- se è un **messaggio in ingresso** verifica la correttezza della firma (attraverso il modulo HSM) e la validità del messaggio (provenienza da un dominio certificato), effettua il delivery verso la mailbox di destinazione attraverso il protocollo LMTP e, una volta consegnato il messaggio crea la ricevuta di avvenuta consegna che l'MTA invierà al mittente del messaggio originale. Nel caso di non validità del messaggio genera un messaggio di anomalia di trasporto che inoltra verso la mailbox dell'utente.

I Log del sistema hanno valore giuridico e verranno mantenuti in appositi storage per il periodo previsto.

Il prodotto è stato progettato in modo tale da essere modulare, così da permettere future estensioni ed adattamenti.

	<i>OpenPEC: La soluzione open source per la Posta Elettronica Certificata</i>
	<i>OpenPEC-descrizione-sito</i>

Prodotti utilizzati

La soluzione sopra descritta può essere realizzata utilizzando esclusivamente prodotti open source non sottoposti a costi di licenza, quali Postfix, OpenLDAP, Courier, CLAMAV, Squirrelmail.

Tali prodotti, tutti collaudati e stabili, assicurano al cliente indiscutibili vantaggi sia in termini economici che pratici e gli consentono di raggiungere in breve tempo una sensibile riduzione dei costi e l'indipendenza dai fornitori senza rinunciare ad un supporto tecnico professionale ed affidabile.

Bibliografia

- [1] Decreto del Presidente della Repubblica del 28/12/2000
<http://www.interlex.it/testi/dpr00445.htm>
- [2] Decreto del Presidente della Repubblica del 11/2/2005
http://www.cnipa.gov.it/site/_files/DPR%2011%20febbraio%202005%20n.68.pdf
- [3] Decreto del Presidente del Consiglio dei Ministri (DPCM):
http://www.cnipa.gov.it/site/_files/DMxPEC2.pdf
- [4] Regole Tecniche del servizio di trasmissione di documenti informatici tramite PEC:
http://www.cnipa.gov.it/site/_files/PEC%20All.pdf
- [5] Schema circolare per la richiesta di accreditamento quale gestore di PEC:
http://www.cnipa.gov.it/site/_files/Circolare%20Accr.%20PEC.pdf
- [6] sito OpenPEC (approfondimenti sulla soluzione):
<http://www.openpec.org/>