

OpenPEC: La soluzione open source per la Posta Elettronica Certificata

*Descrizione della soluzione
White paper*

Autore	EXEntrica srl
Versione	1.5
Data	17/10/2008

Glossario

Open Source	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.
MTA	Mail Transfer Agent. E' un modulo che ha il compito di effettuare il dispatching dei messaggi di posta elettronica (invio e ricezione)
LDAP	<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.
SMTP	Simple Mail Transfer Protocol. Protocollo Standard per la trasmissione di email su internet
SMTP/S	SMTP con autenticazione sicura
POP	<i>Post Office Protocol</i> . Protocollo per l'accesso ad un account di posta elettronica
POP/S	POP con autenticazione sicura
IMAP	Internet Message Access Protocol. Protocollo per l'accesso ad un account di posta elettronica e per la lettura delle email.
IMAP/S	IMAP con autenticazione sicura
LMTP	<i>Local Mail Transfer Protocol</i> . Derivato dall'SMTP, lo può sostituire nei casi in cui il ricevente non gestisce la coda dei messaggi.
HSM	<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.

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.

Il funzionamento del “sistema PEC” si basa sul concetto di **Gestori di PEC**, enti pubblici ed aziende private che, una volta ottenuta una certificazione da parte del CNIPA (Centro Nazionale per l'Informativa nella Pubblica Amministrazione), hanno la possibilità di erogare il servizio e di rivendere caselle e domini PEC.

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]. A partire da questa data i soggetti pubblici e privati possono richiedere di certificarsi quali fornitori del servizio di PEC.
- Il 7 dicembre 2006 viene emessa la circolare CNIPA n.51 che descrive le modalità di “Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata” da parte del CNIPA stesso.

Come funziona un sistema di PEC

Il funzionamento di un sistema di Posta Elettronica Certificata può essere descritto sulla base dello schema di seguito riportato.

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.

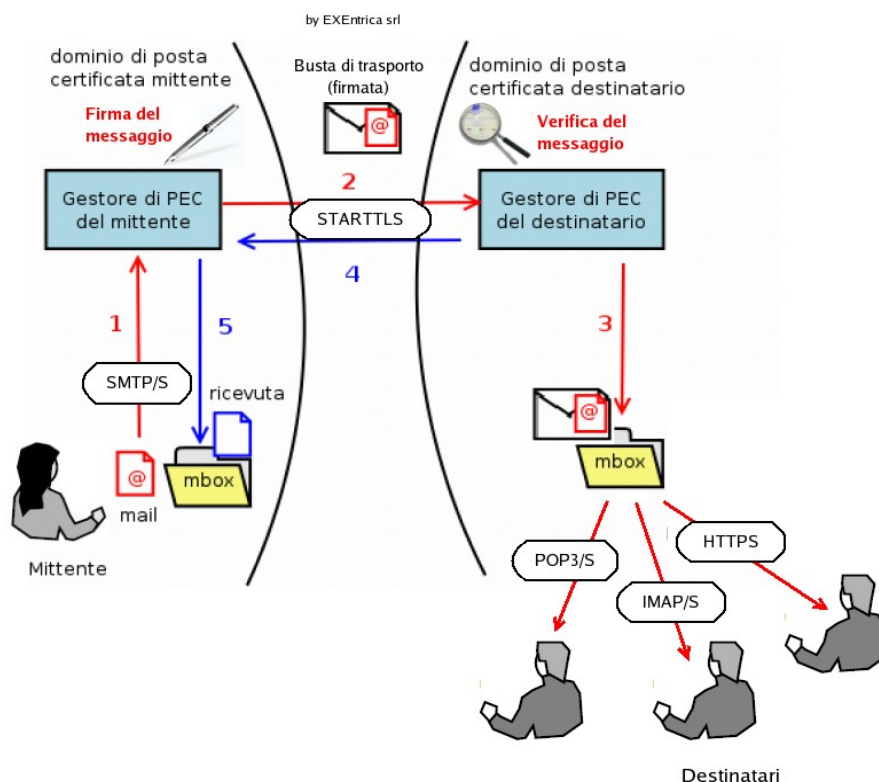


Figura 1 - Funzionamento di un sistema di PEC

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.

Che cosa cambia per l'utente finale

L'utente finale vede la casella di PEC come una normale casella di posta elettronica. Sono sufficienti alcune banali configurazioni per aggiungere l'account di posta certificata ai principali client sul mercato (Outlook, Outlook Express, Thunderbird, Eudora, etc.).

Le sole differenze percepite dall'utente sono a livello funzionale. Ad esempio, in mancanza di problemi, l'utente riceve, per ogni messaggio inviato:

- una *ricevuta di accettazione* da parte del proprio gestore (che certifica che il messaggio spedito è corretto);
- una *ricevuta di avvenuta consegna* (che certifica che il 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 PEC.

Per diventare gestore 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 accreditamento che prevede:

- la messa in opera del sistema;
- la redazione di una serie di documenti amministrativi e tecnici che descrivano la struttura societaria ed organizzativa del candidato, le modalità di erogazione del servizio, l'architettura della soluzione, il piano di sicurezza adottato, i flussi operativi implementati, etc;
- l'esecuzione dei test di interoperabilità;
- l'eventuale visita ispettiva da parte dell'ente certificatore (CNIPA).

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).

OpenPEC non è un sistema di posta elettronica sviluppato completamente da zero ma si propone come estensione di Postfix, uno dei più diffusi mail server Open Source.

OpenPEC è rilasciato con licenza Gnu GPL (General Public License) e non prevede costi di licenza.

Caratteristiche principali:

- Piena compatibilità con la normativa vigente
- Prestazioni elevate
- Affidabilità
- Scalabilità
- Modularità
- Compatibilità con i principali Hardware Security Module (HSM) sul mercato
- 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:

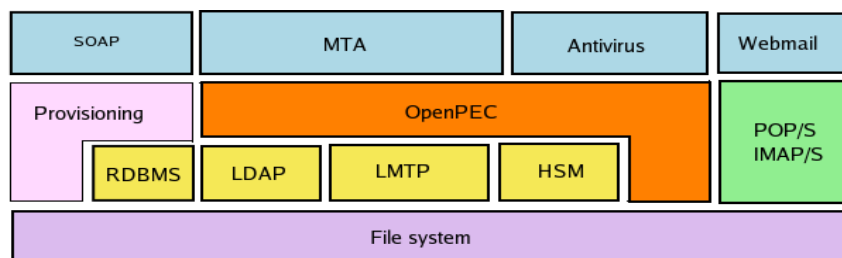


Figura 2 - Componenti del sistema

Come è possibile vedere dallo schema, **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

Prodotti utilizzati

La soluzione descritta utilizza esclusivamente prodotti open source collaudati e testati e non sottoposti a costi di licenza quali **OpenPEC**, **Postfix**, **OpenLDAP**, **Courier-Imap**, **CLAMAV**, **Squirrelmail**.

Bibliografia

[1] *Decreto Legislativo 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali”.*

[2] *Decreto del Presidente della Repubblica N. 445 del 28/12/2000: Testo unico delle*

disposizioni legislative e regolamentari in materia di documentazione amministrativa

- [3] *Decreto del Presidente della Repubblica N. 68 del 11/2/2005*: “Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n.3.
- [4] *Decreto Legislativo del 7 marzo 2005 n. 82*: “Codice dell'Amministrazione Digitale
- [5] *Decreto Ministeriale del 2 novembre 2005*: “Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata”
- [6] *Circolare CNIPA N. 49 del 24 novembre 2005*: 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.
- [7] Sito Openpec (www.openpec.org): approfondimenti sulla soluzione
- [8] Sito Exentrica (www.exentrica.it): offerta per diventare gestori
- [9] Sito GigaPEC (www.gigapec.it) offerta casellePEC, domini certificati e soluzioni personalizzate di posta elettronica certificata)

Informazioni

Exentrica srl
Via Giuntini, 63 - 56023 Cascina (PISA)
tel: +39 050 754.703 - fax +39 050 754.707
email: info@exentrica.it
web: <http://www.exentrica.it>