

Open**PEC**

OpenPEC: la soluzione open source  
per la Posta elettronica certificata

Umberto Ferrara [[ferrara@exentrica.it](mailto:ferrara@exentrica.it)]

Seminario PEC e cooperazione applicativa  
TossLab – Dip Informatica, Università di Pisa  
2 aprile 2009



[::www.exentrica.it](http://www.exentrica.it)  
[::info@exentrica.it](mailto:info@exentrica.it)

## :: OpenPEC ([www.openpec.org](http://www.openpec.org)) ::

- ★ è l'unica soluzione open source di PEC
- ★ è un progetto “nato” open source
- ★ lo sviluppo avviene in forma collaborativa sfruttando le infrastrutture del repository Sourceforge.net ([www.sf.net](http://www.sf.net))
- ★ viene rilasciato con licenza GPL
- ★ non è un sistema monolitico ma si propone come estensione dei principali mail server open source (Postfix)
- ★ è scritto in perl e C
- ★ si basa su un "branch" del progetto Open Source AMaVIS, che estende i mail server più diffusi con funzionalità di antivirus nei messaggi di posta elettronica.



## **:: OpenPEC: un po' di storia::**

- ★ Gen 2004: creazione progetto sul repository SourceForge da parte di Ksolutions spa e da un gruppo di programmatori del progetto OpenCA
- ★ Lug 2004: esce OpenPEC 1.0
- ★ Ago 2004: OpenPEC passa i test di interoperabilità ed ottiene la certificazione (fase sperimentale); nei mesi successivi si certificano una ventina di provider con OpenPEC.
- ★ Nov 2005: viene pubblicato in G.U. Il DM che regola la PEC
- ★ Gen 2006: viene costituita Exentrica che prende in carico la gestione del progetto e lo sviluppo della nuova release
- ★ Set 2006: esce OpenPEC 2.0 conforme alla normativa
- ★ Ott 2006: si certifica il primo gestore con OpenPEC (Aruba PEC spa)
- ★ Da Gen 2007 ad oggi diventano gestori utilizzando OpenPEC una banca (IWBank), una società di servizi (Namirial spa) e una PA (Provincia di Nuoro)

## **:: OpenPEC: principali caratteristiche ::**

- ★ Piena compatibilità con la normativa vigente
- ★ Architettura scalabile e modulare
- ★ Compatibilità con i principali fornitori di Hardware Security Module (HSM)
- ★ Capacità di gestire sistemi con un elevato numero di domini e/o mailbox
- ★ Marcatura temporale e storicizzazione dei log
- ★ Gestione delle Certificate Revocation List (CRL)

## :: OpenPEC: principali caratteristiche ::

### ★ Affidabilità

- ★ 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

### ★ Prestazioni

- ★ Ambiente multi-process basato sulla libreria Net-Server: numero di processi sempre costante
- ★ La rielaborazione di una mail avviene dal punto in cui è stata interrotta

## :: OpenPEC: un po' di dati ::

- ★ Il prodotto ha superato i test di interoperabilità CNIPA
- ★ Tra i **gestori** accreditati: Internet provider, banche, aziende di servizi, PA
- ★ Tra i **clienti**: aziende di servizi, internet provider, università, ordini professionali, liberi professionisti, enti pubblici, privati
- ★ Attualmente OpenPEC gestisce:
  - il **90%** dei domini PEC totali
  - il **50%** circa delle caselle totali
- ★ Utilizzato a livello sperimentale in Università e Centri di ricerca
- ★ Soluzione interamente OS (tutti i prodotti utilizzati sono open)

## :: OpenPEC: i siti di riferimento ::

★ <http://www.openpec.org>

★ <http://sourceforge.net/projects/openpec/>



**SOURCEFORGE.NET** Log in Create account Community Help Search

OpenPEC Summary Tracker Download More

The OpenPEC project is a collaborative effort to develop an Open Source Certified E-Mail System (in Italian: Posta Elettronica Certificata or PEC) as required by the Italian law. See the CNIPA site for details (<http://www.cnipa.gov.it>)

Download openpec - 2.2.0

**Posta Elettronica Certificata**  
- Open Source Project -

OpenPEC K solutions EXENTRICA professional open source SOURCEFORGE.NET

Il progetto Documentazione Download Community

Cerca nel sito Powered by Google Cerca

**Rilasciato OpenPEC 2.2**

**Rilasciata la versione 2.2 di OpenPEC**  
OpenPEC-2.2.0 recepisce tutte le ultime note ed aggiornamenti emessi dal CNIPA e aggiunge un approccio nuovo per la comunicazione verso i moduli HSM con l'obiettivo di migliorarne l'affidabilità ed aumentare la velocità nelle operazioni di firma e verifica. Viene infine semplificata la configurazione, migliorato il log con l'aggiunta di una traccia di profiling per l'ottimizzazione del sistema ed, ovviamente, eliminati alcuni bug.

- :: le novità
- :: download

**Introduzione**

- :: Cosa c'è da sapere
- :: La normativa ufficiale
- :: OpenPEC su SF.net
- :: Architettura e caratteristiche
- :: Documentazione
- :: Scarica il software ora
- :: Iscriviti alle mailing list

**Offerte commerciali**

**K solutions** Ksolutions S.p.A., l'azienda fondatrice del progetto, fornisce servizi di PEC direttamente o tramite terzi. Per informazioni: [info-at-ksolutions.it](mailto:info-at-ksolutions.it)

**EXENTRICA** EXENTRICA S.r.l., costituita dal team di sviluppo, realizza sistemi "chiavi in mano" di posta elettronica certificata seguendo il cliente fino al conseguimento della certifica di "gestore di PEC". Per informazioni: [info-at-exentrica.it](mailto:info-at-exentrica.it)

**GIGAPEC** GigaPEC Acquista subito una casella di posta elettronica certificata su dominio [gigapec.it](http://gigapec.it) soli **5 euro** + IVA. Con la tua casella di posta elettronica certificata potrai inviare email con la stessa validità legale delle raccomandate A/R.

News Details Public Activity

Project Admins : [emiliaus](#), [flazan](#), [giova23](#), [luca76](#), [lucadex](#), [madwolf](#), [uferrara](#)

Developers : [10](#)

Development Status : [5 - Production/Stable](#)

Intended Audience : [System Administrators](#), [Customer Service](#), [Legal Industry](#)

License : [GNU General Public License \(GPL\)](#)

Operating System : [OS Independent \(Written in an interpreted language\)](#)

Programming Language : [Perl](#)

Topic : [Filters](#), [Mail Transport Agents](#)

Translations : [Italian](#)

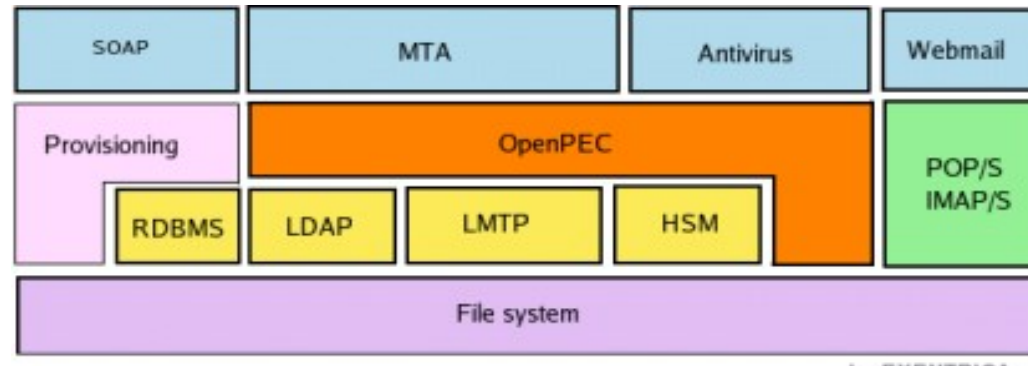
User Interface : [Non-interactive \(Daemon\)](#), [Web-based](#)

Project UNIX name : openpec

Registered : 2003-08-11 11:35

## :: architettura di una soluzione basata su OpenPEC ::

l'architettura è modulare e scalabile

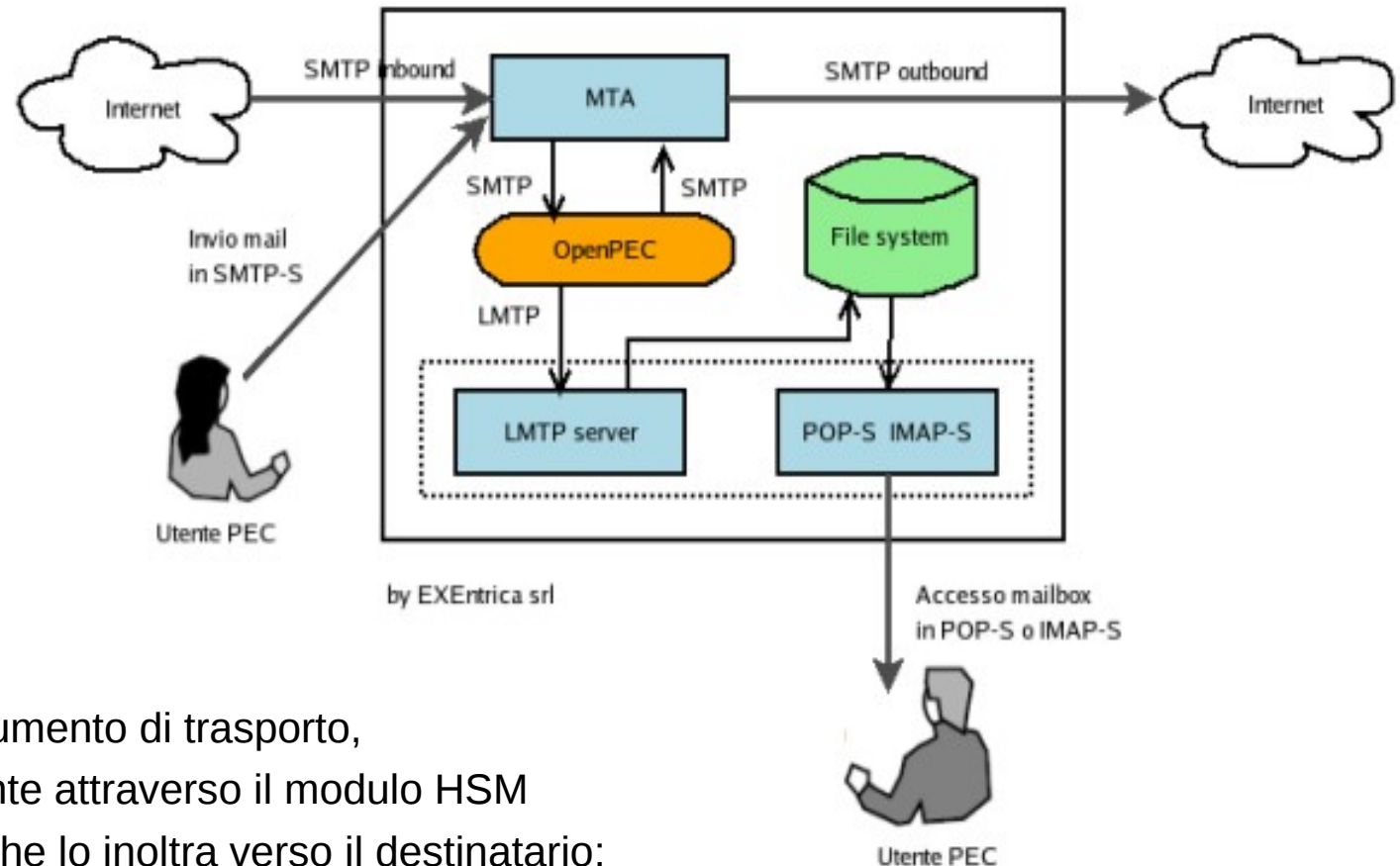


- ★ modulo Antivirus,
- ★ Mail Transfer Agent (MTA): "routing" e "dispatching" delle mail
- ★ server LDAP: mirror dell'indice dei gestori CNIPA
- ★ database (RDBMS): account di posta
- ★ server LMTP: "delivery" dei messaggi nella mailbox degli utenti
- ★ Modulo per la firma dei messaggi attraverso i dispositivi HSM (Hardware Security Module)
- ★ storage (file system): memorizzazione delle mailbox e dei log di sistema
- ★ server POP-IMAP: accesso alle caselle attraverso client
- ★ modulo di provisioning: creazione/modifica degli account
- ★ webmail: consultazione delle caselle attraverso i più comuni internet browser

## **:: la soluzione utilizza solo prodotti open source ::**

- ★ MTA: Postfix
- ★ POP/IMAP: Courier-Imap, Cyrus
- ★ Webmail: Squirrelmail
- ★ Antivirus: ClamAv
- ★ LDAP: OpenLDAP
- ★ DB: mySql

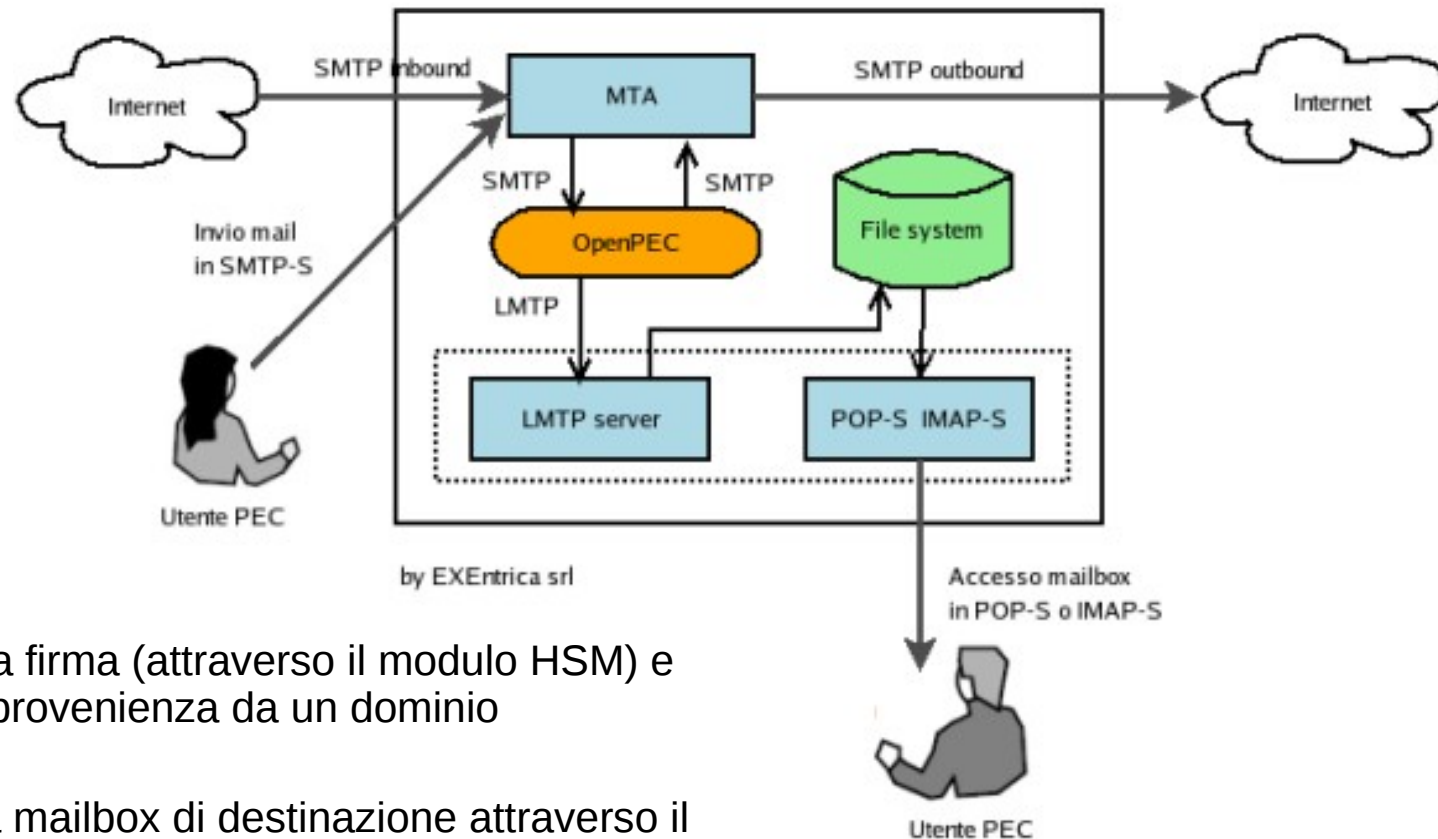
## :: funzionamento OpenPEC: msg in uscita ::



### messaggio in uscita:

- ★ lo incapsula in un documento di trasporto,
- ★ lo firma elettronicamente attraverso il modulo HSM
- ★ lo restituisce all'MTA che lo inoltra verso il destinatario;

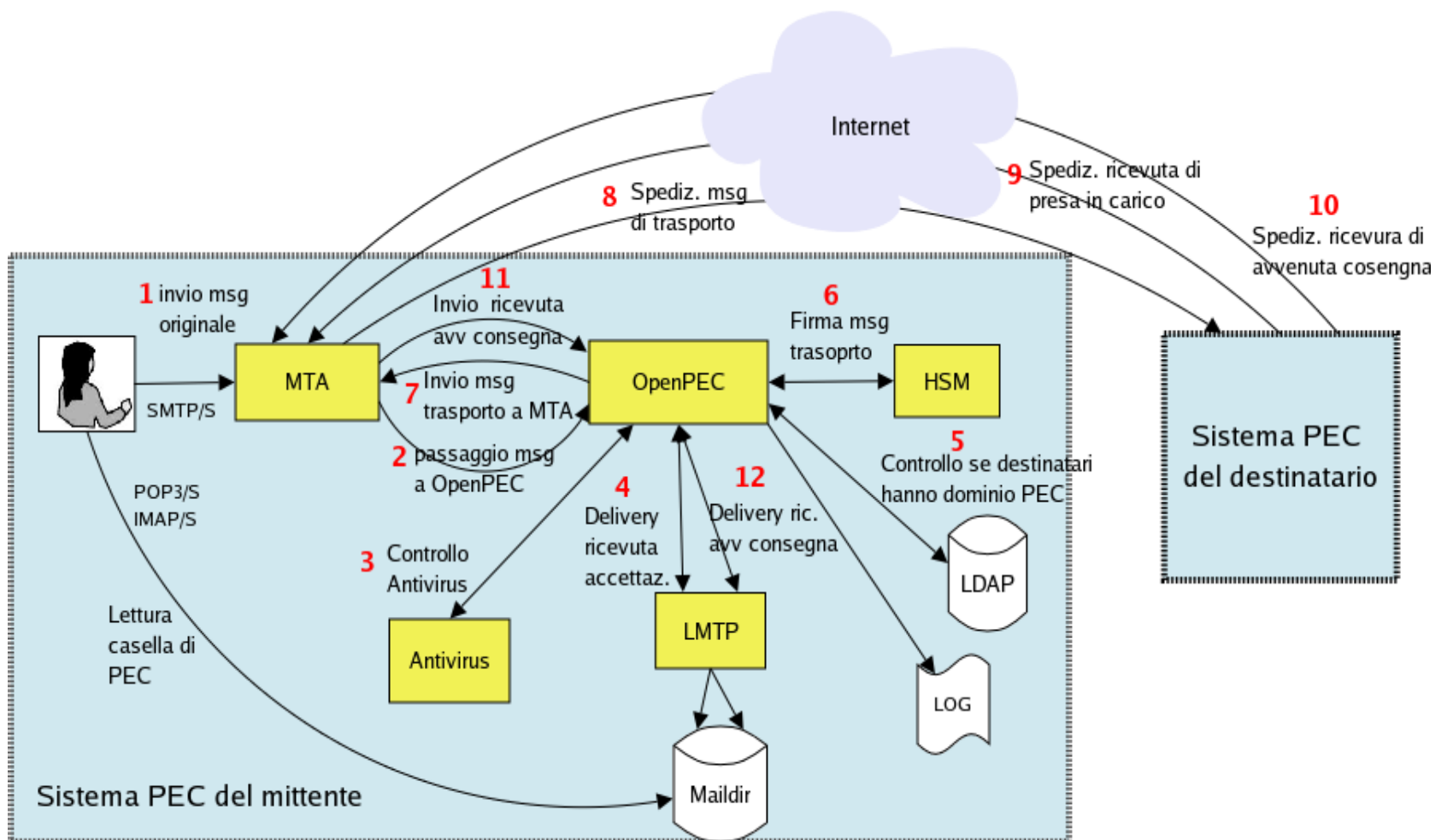
## :: funzionamento OpenPEC: msg in ingresso ::



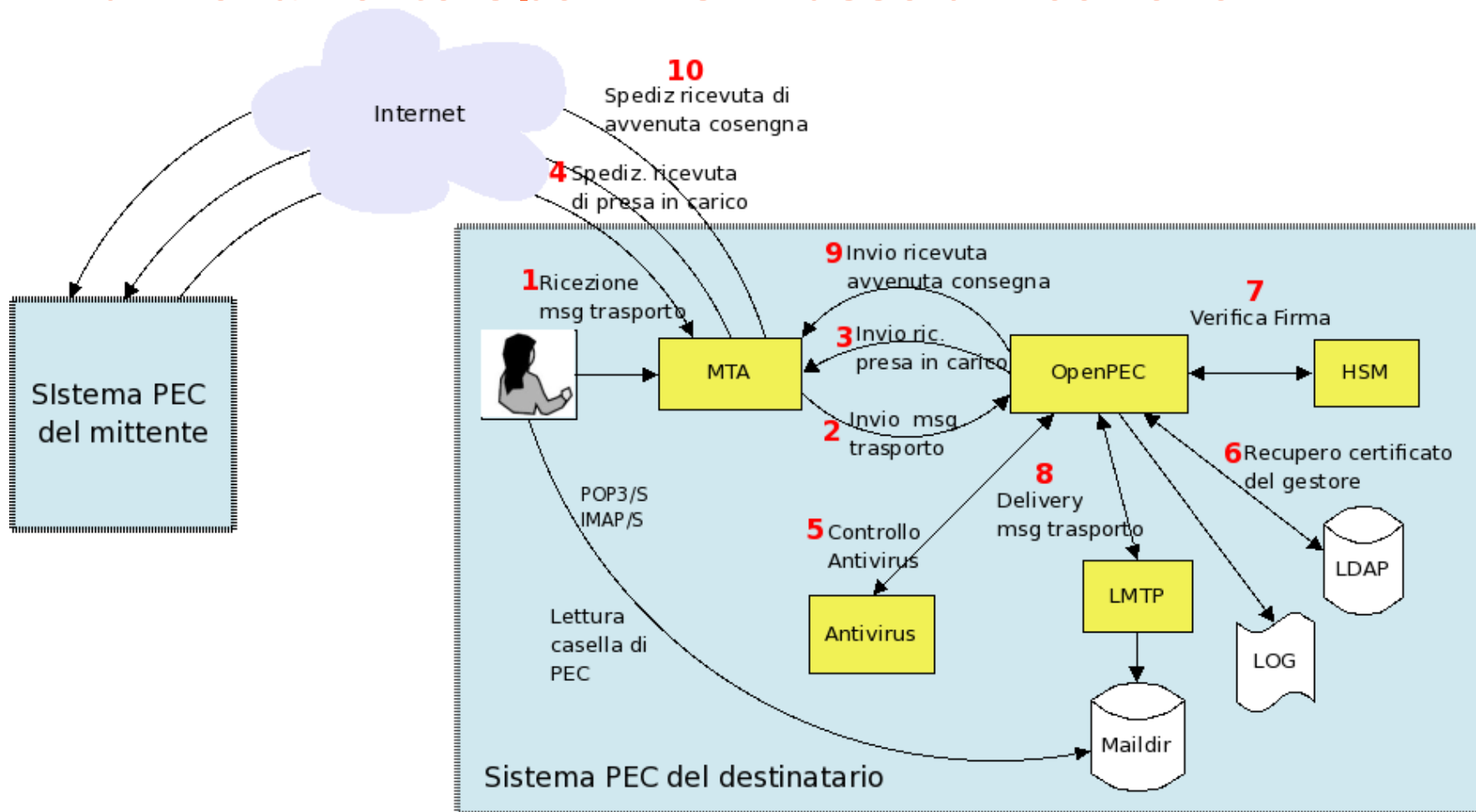
### **messaggio in ingresso:**

- ★ 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 LMT
- ★ crea la ricevuta di avvenuta consegna che l'MTA invierà al mittente

## :: funzionamento OpenPEC: flusso di invio ::



## :: funzionamento OpenPEC: flusso di ricezione ::



## :: scheduler ::

Lo scheduler viene utilizzato per tutte le operazioni che devono essere eseguite a seguito del verificarsi di eventi temporali. Ad esempio:

- ★ Rotazione dei log (eventii temporali o di dimensione dei file)
- ★ Generazione avvisi di mancata consegna per superamento tempo massimo

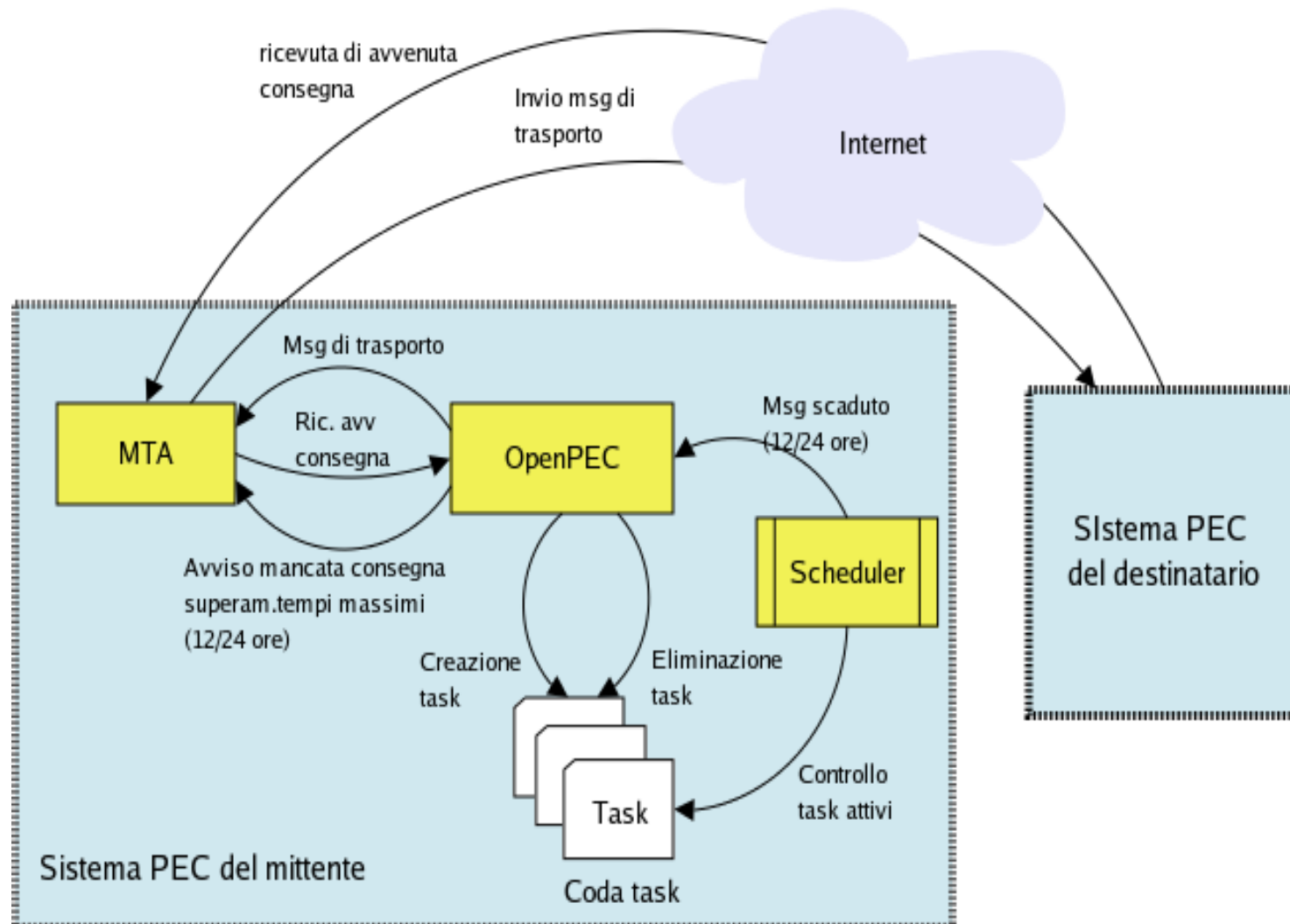
Ogni task è un file memorizzato su file system condiviso

E c ontiene:

- ★ Id del task
- ★ Scadenza
- ★ Operazione da eseguire

Le operazioni vengono svolte da OpenPEC

## :: funzionamento OpenPEC: scheduler ::



## :: interazione OpenPEC-Postfix ::

### Mail PEC in ingresso:

- ★ Tutte le mail in ingresso vengono redirette da postfix verso la porta 10024 di OpenPEC.
- ★ OpenPEC mantiene aperta la comunicazione con Postfix (10024) fino a che non ha portato a termine l'elaborazione della mail in modo tale che in caso di errore la mail rimane nella coda di Postfix e rielaborata successivamente senza alcuna perdita.

### Mail PEC in uscita:

- ★ Postfix rimane in ascolto sulla porta 10025 (ad accesso controllato) per accettare mail da OpenPEC ed inoltrarle verso domini esterni.

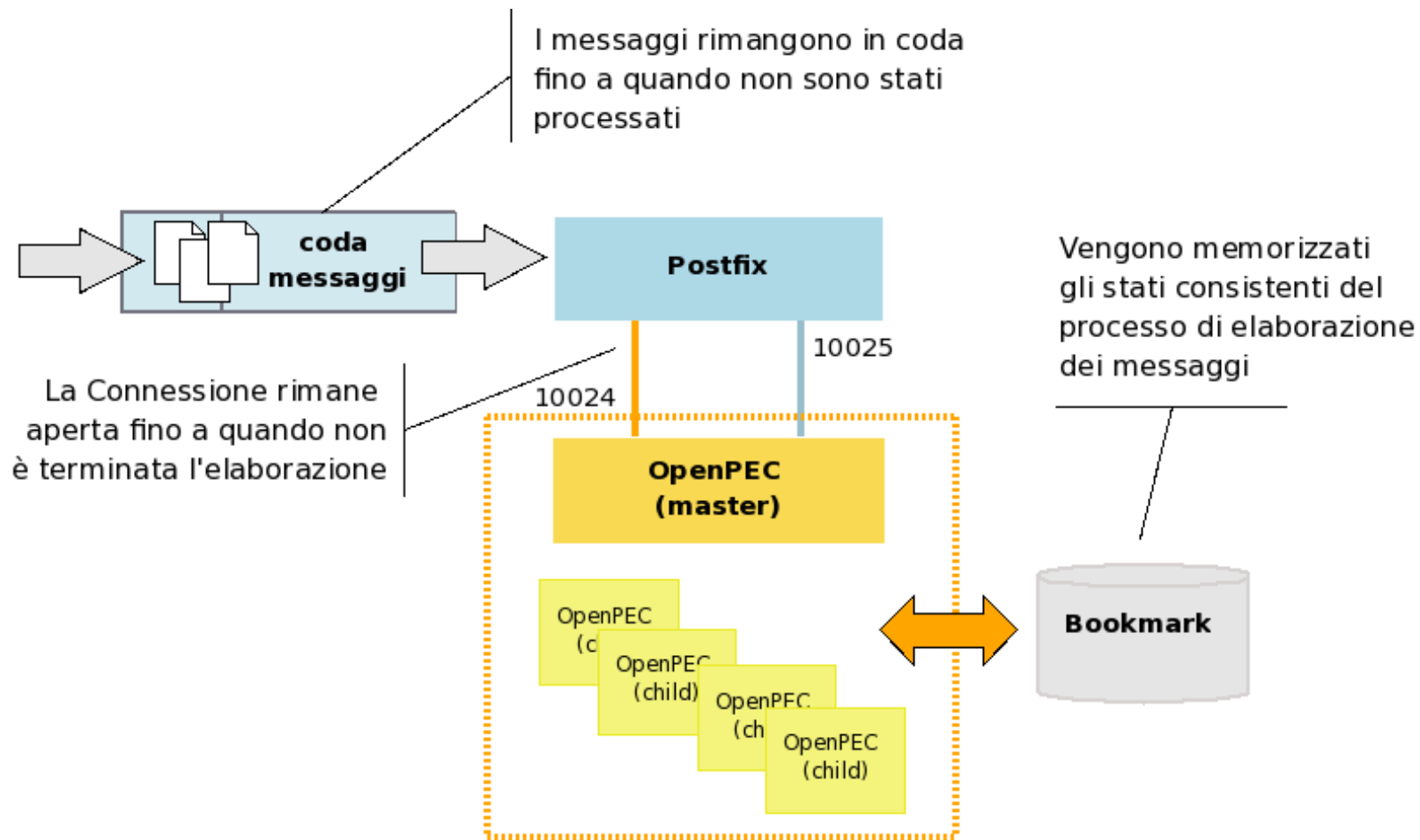
## :: OpenPEC ::

- ★ 1 processo master + n processi figli
- ★ Numero costante di processi figli ognuno dei quali è preposto all'elaborazione di una sigola mail per volta.
- ★ Ogni processo figlio ha un tempo di vita predeterminato
- ★ E' in ascolto sulla porta 10024 (smtp) dove riceve le mail.
- ★ Spedisce le mail dirette verso l'esterno tramite la porta 10025.
- ★ Spedisce le mail dirette localmente attraverso la porta 24 (lmtmp).
- ★ Parla con la TSA per la generazione della marca temporale da apporre quotidianamente sui file di log.

## :: OpenPEC ::

- ★ Ha il compito di incapsulare il messaggio originale in un documento di trasporto, firmare e verificare mail certificate esterne parlando con il modulo HSM.
- ★ Parla con il sistema di antivirus per verificare la posta in arrivo al punto di accesso e al punto di ricezione.
- ★ Parla con l'indice della PEC (LDAP mirror) per stabilire su un utente è certificato e per recuperare i certificati utilizzati nel processo di verifica.
- ★ Parla con lo scheduler per eseguire i task esterni (spedire eventuali avvisi di mancata consegna per timeout o per la rotazione dei log con criterio temporale).

## :: fault tolerance ::



## :: OpenPEC: download e prerequisiti ::

### ★ Download:

★ <http://www.openpec.org/download.shtml> Oppure

★ [http://sourceforge.net/project/showfiles.php?group\\_id=87668](http://sourceforge.net/project/showfiles.php?group_id=87668)

### ★ Prerequisiti:

★ S.O.: Linux (è stato testato su RH e Centos)

★ Moduli perl: Crypt::SMimeEngine 0.01, Net::Server 0.94, Sys::SigAction 0.06, MailTools 1.74, Net::SMTP 2.26, Unix::Syslog 0.99, IO::Stringy 2.100, MIME-Base64 3.07, MIME::Tools 5.411, IO::File, Net::LDAP 0.26, File::Basename 2.06, Storable 2.08, Fcntl, Time-HiRes 1.49, libwww-perl-5.805

## :: OpenPEC: installazione ::

1. Creare un gruppo dedicato all'esecuzione di OpenPec. Non dovrebbe essere un gruppo di sistema o essere utilizzato da altri mailer (es. dopec).
2. Creare un account dedicato all'esecuzione di OpenPec. Non dovrebbe essere un utente di sistema o già utilizzato (es. dopec).
3. Download del software
4. Creare una nuova directory ed esplodere quanto scaricato.
5. Procedere digitando quanto segue:

*perl Makefile.PL*

*make test*

*make install*

## :: OpenPEC: configurazione ::

file `/etc/opeconf` (formato: codice Perl)

- ★ CONFIGURAZIONE GENERALE
- ★ CONFIGURAZIONE DEMONI
- ★ ANTIVIRUS
- ★ LOGGING
- ★ CONFIGURAZIONE SMIME
- ★ CONFIGURAZIONE CONNESSIONE LDAP
- ★ CONFIGURAZIONE CONNESSIONE TSA
- ★ TEMPLATE RICEVUTE

## :: OpenPEC: esecuzione ::

*perl [-c configfile] [start | stop | suspend | debug ]*

- ★ **start:** start OpenPEC (modalità standard)
- ★ **stop:** stop OpenPEC
- ★ **suspend:** start OpenPEC in modalità “auto-sospensione”
- ★ **debug:** start OpenPEC in modalità debug
  - ★ 1 solo processo
  - ★ Output su STDERR
  - ★ Per debugging: `perl -d opec debug`

## :: OpenPEC: file di log ::

### Legal (ufficiali):

- ★ Contengono la traccia delle operazioni previste dalla normativa
- ★ Devono essere salvati e marcati (con marcatura di una TSA riconosciuta) ogni 24 ore max
- ★ Devono essere conservati almeno per 30 mesi (conservazione sostitutiva)

### System

- ★ Contengono la traccia di ulteriori informazioni che possono essere utilizzate per monitorare il funzionamento di OpenPEC