

Convegno **Salpa 2004**

OpenPEC

Posta Elettronica Certificata Open Source

Luca De Santis – Flavio Fanton – Luca Manganelli - Emilio Marcheselli

Ksolutions S.p.A.

Relazione presentata al *Salpa 2004* da: Luca De Santis

Abstract

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

La posta certificata implementa una serie di servizi che garantiscono l'avvenuta consegna di un messaggio elettronico ad un destinatario. Il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 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.

OpenPEC vuole essere il primo sistema Open Source di posta elettronica certificata conforme alle linee guida CNIPA. Il progetto, fondato dall'azienda Ksolutions di Pisa, viene rilasciato con una licenza di utilizzo GNU General Public License. Il suo sviluppo avviene in forma collaborativa sfruttando le infrastrutture del sito Sourceforge.net.

L'obiettivo della presentazione è quello di far conoscere il progetto alle PA italiane per incoraggiarle a contribuire alla sua realizzazione, uso e diffusione. Al contempo si vuole sottolineare la validità del modello di sviluppo Open Source per le PA in quanto esso rappresenta una soluzione tecnologicamente valida, accessibile da un punto di vista economico e soprattutto, in quanto "aperta", estendibile, migliorabile e riutilizzabile.

Relazione

Introduzione

L'istituzione della posta elettronica certificata (PEC) risponde all'esigenza di gestire la trasmissione di un documento informatico in una forma che assicuri e certifichi dal punto di vista legale l'avvenuta consegna. Nei casi consentiti dalla legge esso equivale alla notificazione per mezzo della posta "tradizionale" (es. tramite raccomandata con ricevuta di ritorno).

Il servizio si appoggia al protocollo standard di trasmissione della posta elettronica SMTP: gli applicativi "server" coinvolti vengono estesi per implementare opportunamente le linee guida del CNIPA. E' previsto che la mail originale venga incapsulata, utilizzando il formalismo MIME, in un messaggio "contenitore" (detto *messaggio di trasporto*), preparato automaticamente dal server di posta certificata del mittente (o *punto di accesso*) e che include anche i *dati di certificazione*, ovvero gli estremi del messaggio originale codificati in un formato opportuno. Per garantire l'integrità e la non modificabilità dei dati il *punto di accesso* provvede a firmare digitalmente il *messaggio di trasporto*. La firma apposta sul messaggio dal sistema mittente è verificata all'arrivo sul server di destinazione.

Nell'ambito del processo di trasmissione del messaggio vengono generate delle ricevute, trasmesse al mittente, che servono a tener traccia del passaggio delle informazioni tra i vari server. In particolare una prima *ricevuta di accettazione* viene generata dal *punto di accesso* a fronte dell'invio di un messaggio di posta certificata. La *ricevuta di avvenuta consegna* viene invece generata dal server del destinatario (o *punto di consegna*) contestualmente all'avvenuto delivery del messaggio nella casella di posta elettronica del ricevente: questa ricevuta testimonia l'avvenuta consegna del messaggio (ma non ovviamente la lettura da parte del destinatario) e certifica la data e l'ora in cui questa è avvenuto.

Se il mittente e il destinatario risiedono su server PEC diversi una terza ricevuta viene generata in un istante compreso fra quello delle due precedenti. Si tratta della *ricevuta di presa in carico* che attesta l'avvenuta ricezione del messaggio del server destinatario (in questo caso si parla di *punto di ricezione* visto che questa entità potrebbe differire dal *punto di consegna* vero e proprio), in una fase quindi antecedente al delivery nella casella del destinatario. In questo caso la ricevuta, sempre implementata mediante un messaggio di posta elettronica, viene inviata al server del mittente.

Tutte queste ricevute sono sempre firmate elettronicamente dai rispettivi server mittenti.

Dal punto di vista della sicurezza è previsto che gli utenti si colleghino utilizzando protocolli di trasmissione sicuri (basati su SSL) verso i rispettivi server sia per l'invio (SMTP-TLS) che per la lettura dei messaggi (POP-S, IMAP-S). Il *messaggio di trasporto* non è cifrato, così come non è cifrato il protocollo di trasmissione tra server che è lo standard SMTP.

Nel caso di invio di messaggi verso server non PEC il destinatario riceverà il *messaggio di trasporto* come se fosse un utente PEC, mentre il mittente non riceverà nessuna *ricevuta di consegna*. Quando invece un messaggio inviato da un server convenzionale (non PEC) viene ricevuto da un server PEC, questo viene "imbustato" in un *messaggio di anomalia di trasporto* che ne evidenzia la provenienza non certificata insieme ai dati del server di ricezione.

Le firme digitali poste automaticamente dai server PEC nei vari messaggi (di trasporto o ricevute) devono essere conformi alla normativa vigente, pertanto devono essere utilizzati certificati erogati da *Certification Authority* riconosciute.

Presso il CNIPA è mantenuto un repository centrale (sotto forma di server LDAP) in cui sono presenti i dati di tutti i server PEC attivi, che deve essere interrogato automaticamente per permettere la verifica delle firme e della validità dei messaggi.

I sistemi di posta elettronica certificata devono anche implementare politiche di logging sicure. Particolare attenzione deve essere poi posta alla gestione di questi log, in modo da garantire la riservatezza delle informazioni in essi memorizzate e la sicurezza, ovvero l'autenticità e l'inalterabilità nel tempo: è infine previsto che i gestori del servizio debbano conservare questi log per un periodo di almeno due anni e che possano renderli disponibili al CNIPA, a fini ispettivi, o in caso di contenzioso, ai soggetti incaricati di effettuare il controllo.

Le pubbliche amministrazioni ed i privati che intendano esercitare l'attività di gestore di posta certificata devono inoltrare alla Presidenza del Consiglio dei Ministri, Dipartimento per l'innovazione e le tecnologie, domanda di iscrizione nell'indice dei gestori di posta certificata.

I sistemi server PEC devono essere validati dal CNIPA, che ha fornito sul suo sito un insieme di test d'interoperabilità, per verificare la conformità del sistema nelle interazioni con le architetture già approvate.

OpenPEC: il progetto

Attualmente le PA possono avvalersi dei servizi di PEC in due forme, o acquistando opportuni prodotti commerciali o usufruendo del servizio erogato in outsourcing. In entrambi i casi si trovano nella necessità di fare degli investimenti a costi di mercato, senza alcun controllo diretto sul servizio.

Nella maggior parte dei progetti di eGovernment presentati negli ultimi anni si fa un'esplicita richiesta di soluzioni Open Source o comunque vi è la richiesta di fornitura dei sorgenti dei progetti software prodotti dai fornitori. Questa tendenza è giustificata dalla necessità di avere un controllo diretto sui pacchetti software utilizzati, di garantirsi un possibile sviluppo anche in assenza del produttore originale, di diminuire i costi delle licenze e del mantenimento del software e di poter condividere con la comunità delle PA i prodotti acquistati o creati con il denaro pubblico.

I servizi di PEC, così come quelli del Protocollo Informatico, sono da considerarsi componenti essenziali e basilari di tutti i sistemi informativi delle PA moderne: devono quindi essere di facile accesso sia dal punto di vista del costo che del loro mantenimento.

Sulla base di queste e di altre considerazioni Ksolutions ha deciso di dare vita in modalità Open Source al progetto OpenPEC. OpenPEC può rappresentare una soluzione ideale per le PA di ogni dimensione, a partire quindi dalle più piccole che vedono così abbattuti i costi di accesso per poter implementare una soluzione di posta certificata. La licenza scelta per OpenPEC è la GNU General Public License (GPL) scelta che apre lo sviluppo del progetto a tutti coloro – aziende, PA, sviluppatori – che vogliono contribuire alla realizzazione della prima implementazione Open Source di un sistema PEC.

OpenPEC nasce ufficialmente nell'estate del 2003, con l'iscrizione del progetto presso il sito SourceForge.net. Nel marzo 2004 è previsto il rilascio della prima versione Beta. La homepage del progetto è <http://www.openpec.org>.

OpenPEC: le soluzioni tecniche

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 *qmail*, 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.

I messaggi scambiati tra sistemi di PEC sono firmati elettronicamente, per questo OpenPEC utilizza il sistema PKI di OpenCA, un altro progetto Open Source italiano (cfr. <http://www.openca.org/>) che si basa sull'estensione dei moduli OpenSSL. Le componenti di OpenPEC che gestiscono la firma e il controllo dei messaggi sono integrati nativamente con OpenCA: non è comunque escluso l'utilizzo di altri sistemi PKI, in particolare di quelli dei fornitori iscritti come "Certificatori" nell'elenco pubblico tenuto dal CNIPA.

OpenPEC è sviluppato nel linguaggio Perl, scelto per le sue funzionalità avanzate di gestione e manipolazione di testi. E' stato progettato in modo tale da essere modulare, così da permettere future estensioni e adattamenti. Da un punto di vista implementativo OpenPEC è basato su un "branch" del progetto Open Source AMaVIS¹, che estende i mail server più diffusi con funzionalità di scansione dei virus contenuti come allegati nei messaggi di posta elettronica.

Per garantire la massima compatibilità con i più diffusi MTA (Mail Trasfert Agent), l'interfaccia di comunicazione è realizzata mediante implementazione di un gateway SMTP e l'utilizzo di "pipe" Unix. La scelta di adottare un ambiente multi-process rende inoltre il plug-in meno invasivo in termini di tempo di elaborazione dei messaggi: all'avvio il server OpenPEC genererà un *pool* prestabilito e configurabile di processi e si occuperà di mantenere il loro numero costante per non appesantire il carico complessivo della macchina.

L'affidabilità è garantita salvando immediatamente la mail su un file temporaneo e mantenendo la comunicazione aperta con l'MTA fino ad elaborazione ed eventuale dispatching ultimati: in caso di errori o di chiusura erronea della comunicazione, l'MTA provvederà a recuperare la mail e rielaborarla successivamente mediante il suo sistema di code.

I codici sorgenti di OpenPEC sono disponibili sul sistema CVS di Sourceforge.net. Nel marzo del 2004 è previsto il rilascio di una prima versione beta del software integrata ad almeno un sistema di posta elettronica Open Source. Informazioni aggiornate e dettagliate sul progetto sono reperibili alla url <http://www.openpec.org>.

¹ Il progetto branch è AMaVIS-new la cui home page è <http://www.ijs.si/software/amavid>.