



PEC: POSTA ELETTRONICA CERTIFICATA

Marco Caggiano

Finalmente è possibile inviare e-mail che hanno valore legale, allo stesso modo di una raccomandata con ricevuta di ritorno. Lo strumento di comunicazione ideale per aziende, professionisti e privati

L'e-mail è da tempo uno dei mezzi di comunicazione più utilizzati per la sua elevata efficienza. Privati, aziende e professionisti di ogni genere l'hanno ormai sostituita alla posta tradizionale. A tale proposito, finalmente, anche in Italia è da poco diventata uno strumento di comunicazione con validità legale, grazie alla nascita della cosiddetta **PEC, Posta Elettronica Certificata**. La PEC risolve, in un colpo solo, i problemi di validità legale e affidabilità della posta elettronica tradizionale. Inoltre, si ha a disposizione uno strumento mediante il quale è possibile assicurarsi che mittente e destinatario dell'e-mail siano autentici senza ombra di dubbio, e che il ricevente abbia letto o almeno aperto il messaggio inviato. In effetti, la PEC ha lo stesso valore legale della raccomandata con ricevuta di ritorno della posta tradizionale, quindi può sostituire a tutti gli effetti quest'ultima per l'invio di documenti importanti, pagamenti, contratti, ecc. I sistemi di posta elettronica certificata esistono già da tempo, uno dei più noti è **Thawte**, fondata da Mark Shuttleworth, proprietario di Canonical Ltd e finanziatore di Ubuntu. Ma la novità in Italia è che per la prima volta la PEC è riconosciuta e sostenuta dallo stesso stato con una propria infrastruttura. Per legge, non è obbligatorio utilizzare la PEC statale, va bene qualsiasi altro fornitore, come **Aruba** (www.aruba.it), ad esempio. In sintesi la PEC risolve diversi problemi legati all'uso della posta elettronica tradizionale: ha validità legale, permette l'identificazione sicura di mittente e destinatario, il contenuto dei messaggi è crittografato o comunque certificato mediante la crittografia e le e-mail sono difficili da rintracciare da parte di cracker e pirati informatici in genere.

L'ASPETTO LEGALE

La PEC è obbligatoria per liberi professionisti, imprese ed aziende anche se non vogliono dare validità legale alla loro posta elettronica. Le imprese ed i liberi professionisti, possono indicare il proprio indirizzo di posta elettronica certificato quando si iscrivono nel registro delle imprese, o nel proprio albo professionale. Legalmente nella PEC vengono messi in gioco quattro importanti fattori: **il mittente, il gestore di posta elettronica certificata, il destinatario e il mezzo di trasporto** (ad esempio Internet). Il mittente ed il destinatario possono essere in possesso di un dispositivo

di certificazione hardware, oppure della semplice firma digitale fornita dal gestore, o direttamente gestita da quest'ultimo, in modo trasparente. Il gestore è un organo autorizzato dallo stato, più precisamente dal **CNIPA** (www.cnipa.gov.it/site/it-it/), il **Centro Nazionale Informatica nella Pubblica Amministrazione**, iscritto in un registro, di cui viene certificata l'abilità tecnico-organizzativa, per la gestione dei certificati di posta, e della grande quantità di dati a questa associati. Quest'ultimo, può rilasciare caselle di posta a privati e aziende, con un dominio qualsiasi, deciso dall'utente o prefissato, a pagamento o gratuite, e deve tenere traccia di tutte le operazioni, i certificati e le ricevute di deposito, per almeno 30 mesi, così da assicurare il mittente e il destinatario che in caso di perdita di dati, sia conservato ancora il valore giuridico necessario perché la PEC venga riconosciuta come strumento valido. Le **Posteitaliane** sono l'organo principale scelto per amministrare la PEC attraverso il loro sistema **Postecert** (<http://postecert.poste.it/pec/index.shtml>), che offre una casella gratuita limitata ed altre a pagamento. Poi ci sono i gestori privati, come **Aruba**, il cui servizio PEC è a pagamento, anche se il costo è molto basso utilizzando un loro dominio, mentre aumenta, se si desidera un dominio proprio. Internet di solito è il mezzo principale con cui vengono inviate queste e-mail, anche se nessuno vieta di servirsi di altri mezzi e/o reti. Molto di tutto questo è scritto nel decreto 11 febbraio 2005, n.68, nel decreto ministeriale del 2 novembre 2005 e nelle varie circolari del CNIPA, come la CR/49 del 24 novembre 2005, o del 7 dicembre 2006. Purtroppo, la PEC non è uno standard internazionale, come altri sistemi, che comunque si possono utilizzare e, quindi, rimane un qualcosa di italiano che, insomma, all'estero ha poco valore.

COME FUNZIONA

La posta elettronica certificata funziona attraverso un sistema di chiavi pubbliche e private, praticamente utilizzando la **crittografia a chiave asimmetrica**. Ogni individuo possiede: una chiave privata, una pubblica e una firma ottenuta inserendo come parametri nell'algoritmo di cifratura, una chiave privata e il messaggio. Quando si invia l'e-mail, il soggetto ricevente, utilizzando un algoritmo specifico, verifica la sua autenticità

La PEC con Thunderbird

Posta elettronica certificata con il client Mozilla

01

NUOVO ACCOUNT

Dopo aver registrato un account PEC, ad esempio su **Aruba** (www.pec.it), apriamo Thunderbird e selezioniamo **File/Nuovo/Account di posta...** Inseriamo l'indirizzo di posta, il nome, il cognome e la password di accesso scelti durante la registrazione. Infine, procediamo premendo su **Continua**. Thunderbird dovrebbe riconoscere automaticamente i server, altrimenti inseriamo i dati manualmente. Possiamo usare sia **IMAP** sia **POP3**.

02

SETUP AUTOMATICO

Per procedere premiamo **Crea account**. Thunderbird controllerà automaticamente la correttezza dei dati inseriti, se tutto è a posto verremo riportati sulla schermata principale del client. In caso contrario bisogna configurare il client manualmente da **Impostazione manuale...** Settiamo le porte POP3 e IMAP a 995 e la porta SMTP a 465. Come crittografia scegliamo **SSL/TLS**. In ogni caso, possiamo già utilizzare la posta PEC.

Per chi usa Evolution

Configurazione del client Gnome per l'utilizzo della PEC

01

ACCOUNT CERTIFICATO

Apriamo Evolution, selezioniamo la voce **Modifica/Preferenze/Aggiungi** e premiamo **Avanti**. Nella nuova schermata, inseriamo nome, cognome e l'indirizzo di posta elettronica certificata. Infine, clicchiamo ancora su **Avanti** per proseguire con la configurazione del client che va eseguita manualmente.

02

SETUP MANUALE

Giunti a questo punto, scegliamo se usare **POP3** o **IMAP**. Nel secondo caso, digitiamo l'indirizzo del server del gestore e quello di posta completo, tipo **nome.cognome@pec.it**, con **Aruba**. Nella sezione **Sicurezza** selezioniamo **Cifratura SSL**, mentre in **Tipo autenticazione** scegliamo **Password**. Procediamo premendo **Avanti**.

03

PEC ABILITATA

Per la posta in uscita, **SMTP**, indichiamo l'indirizzo del server fornito dal gestore e selezioniamo **Il server richiede autenticazione**. In **Sicurezza** scegliamo ancora **Cifratura SSL**, mentre in **Autenticazione** inseriamo come nome utente l'indirizzo di posta certificata e clicchiamo su **Ricorda la password**. Premiamo **Avanti** per terminare il setup.

utilizzando il messaggio stesso, la chiave pubblica e la firma. Ora, poiché la verifica è univoca, basta cambiare uno dei parametri in ingresso, perché non venga accettata la firma e, quindi, l'autenticità del messaggio. Se il messaggio non è lo stesso con cui è stata prodotta la firma, essa non è più valida, stessa cosa per tutti gli altri "elementi" che compongono la

PEC. Ne consegue che si tratta di un sistema estremamente sicuro per la comunicazione e la validazione della stessa tra due individui e organizzazioni. Sebbene sia possibile effettuare attacchi MitM (Man in the Middle), è comunque molto difficile riuscire a far passare come valido un messaggio contraffatto, se non sfruttando eventuali bug delle applicazioni.



Fig. 1 - L'offerta di Aruba per la PEC

Ma il sistema in sé, è già molto sicuro ed affidabile. Come chiave privata, si può anche utilizzare un sistema hardware, ad esempio un lettore di impronte digitali, una pendrive appositamente configurata, una smartcard e qualsiasi tipo di dispositivo hardware dedicato. In rete se ne trovano molti modelli con alcuni specifici per la PEC, forniti, in alcuni casi, dagli stessi gestori. In questo caso si riesce ad identificare univocamente il mittente, ed a gestire molto meglio realtà molto grandi, come le aziende, dando semplicemente ad ogni impiegato una smartcard per la propria PEC, così da sapere chi ha inviato cosa e quando.

COME SI UTILIZZA SU GNU/LINUX?

Per utilizzare la PEC bisogna prima registrare un proprio account, a pagamento o gratuito, presso le Posteitaliane (www.poste.it) o presso un gestore privato, tra cui **Aruba** (Figura 1). Ottenuti tutti i dati, basta configurare il proprio client di posta elettronica (**Thunderbird**, **Evolution**, **KMail**...) con i parametri di connessione forniti dal gestore, quasi come per la posta elettronica tradizionale ed è subito possibile utilizzare la posta elettronica certificata.

TEST DELL'ACCOUNT PEC

Inviando un messaggio, anche alla nostra stessa casella di posta va bene. Noteremo subito che all'avvenuta ricezione, saranno subito inoltrati alla nostra casella di posta, tre e-mail: una riguardante l'accettazione del messaggio, l'altra contenente il messaggio stesso e la terza riguardante la consegna. Noteremo che tutte le informazioni utili, verranno allegate nell'e-mail e nel file **data-cer.xml**, nel caso di **Aruba**. Così non avremo problemi in caso di battaglie legali. Ora ci basterà conservare tutte le e-mail e le notifiche, ed in caso di smarrimento saranno comunque disponibili, sul server per almeno 30 mesi. Nessun problema dunque. In sintesi, la PEC è sicuramente un ottimo mezzo di validazione dei messaggi, tra aziende, ed enti pubblici, anche se, purtroppo, non standardizzata, locale e imposta da leggi che cambiano molto facilmente. Rimane comunque un qualcosa che può aiutarci in determinate situazioni, e la facilità di utilizzo, anche su GNU/Linux, ne fa certamente uno strumento indispensabile. Speriamo che questo articolo sia riuscito a darvi un'idea di cosa sia la PEC, come funziona e utilizzarla con il proprio client. Inoltre, la speranza è di avervi suscitato la curiosità necessaria per approfondire ed informarvi adeguatamente su questo aspetto della legislazione italiana.

Setup di un account PEC su KMail

La procedura per abilitare la posta elettronica certificata sul client KDE



01

INFORMAZIONI ACCOUNT

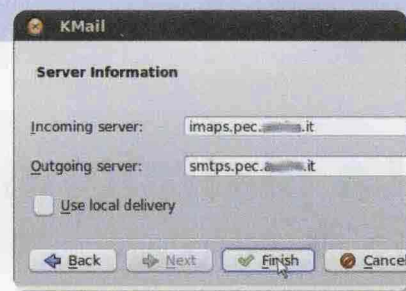
Apriamo KMail, andiamo su Tools/Account Wizard, clicchiamo su **Create a New Identity** e, infine, premiamo **Next**. Nella nuova finestra, selezioniamo **IMAP** (o **POP3**), clicchiamo su **Next** e nella schermata **Account information** inseriamo il nome completo, l'indirizzo di posta elettronica certificata fornitoci dal gestore e il nome della nostra organizzazione. Premiamo **Next**.



02

DATI DI ACCESSO

Nella nuova schermata **Login information**, per prima cosa inseriamo come **Login Name** l'indirizzo di posta elettronica certificata completo. Più in basso, nel campo **Password** digitiamo la password di autenticazione fornitoci dal gestore, nel nostro caso sempre **Aruba**. Fatto ciò, premiamo ancora una volta **Next**. Nella nuova schermata imposteremo i server di posta in entrata e uscita.



03

I SERVER PEC

In **Server information**, per i server di posta in entrata e uscita, **Incoming server** e **Outgoing server** inseriamo i dati di **Aruba**, ad esempio, e premiamo **Finish**. KMail setta automaticamente i parametri di sicurezza. Se la porta SMTP non è 465, andiamo in **Settings/Configure Kmail/Accounts/Sending** selezioniamo l'account PEC e in **Modify/General** impostiamo 465. Tutto qui!