

Posta elettronica certificata e certificati s/mime: differenze e funzionamento

Introduzione alla PEC

La "posta elettronica certificata", meglio conosciuta con l'acronimo PEC, è uno strumento il cui obiettivo è quello di parificare il valore di una e-mail a quello di una raccomandata cartacea con ricevuta di ritorno. Il decreto legge "anticrisi" 185/2008 sembrava ormai aver sancito l'obbligatorietà dell'adozione di una casella PEC da parte di iscritti ad Albi, professionisti ed imprese. In particolare, l'articolo 16 del decreto stabiliva l'obbligo per le imprese di comunicare il proprio indirizzo PEC nella domanda di iscrizione al registro oppure entro un periodo di tempo massimo pari a tre anni, dalla data di entrata in vigore della normativa, per le società già iscritte. I professionisti iscritti ad albi ed elenchi istituiti con legge dello Stato avrebbero invece dovuto comunicare il proprio indirizzo PEC ai rispettivi ordini o collegi entro un anno dalla data di entrata in vigore del decreto legge.

In sede di conversione del decreto legge, sono state da poco apportate numerose modifiche alla versione iniziale dello stesso. Nella sostanza, l'intervento sembra aver rimosso l'obbligatorietà della PEC che è uno standard di matrice italiana. L'impresa od il professionista possono servirsi sì di un indirizzo di posta elettronica certificata (PEC) ma anche, in alternativa, di *"un analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali"*. La modifica applicata alla normativa sembra quindi configurarsi come un'apertura verso l'impiego, in sostituzione della PEC, di tecniche di firma digitale e di tracciamento della consegna equivalenti e gratuite, già disponibili ed utilizzabili mediante l'uso di account di posta di tipo tradizionale ormai da diversi anni.

Vediamo più da vicino in che cosa consiste la PEC e quali soluzioni alternative possano essere utilizzate, anche per certificare il contenuto dei messaggi inviati.

La PEC

Come anticipato, la PEC è stata ideata con l'intento di attribuire al messaggio di posta elettronica lo stesso valore di una raccomandata con ricevuta di ritorno di tipo tradizionale. Tra l'altro, è ormai cosa nota che la raccomandata A/R non possa essere la soluzione definitiva per le problematiche legate alla certezza della ricezione, al non ripudio della stessa, all'attestazione certa dei contenuti della comunicazione nonché alla possibilità di stabilire data ed ora di consegna.

Poiché la raccomandata e/o la ricevuta di ritorno stessa possono perdersi non ci può mai essere la certezza assoluta della ricezione. Proprio per questo motivo il destinatario potrebbe affermare il falso dichiarando di non aver ricevuto alcunché. Per non parlare dei contenuti della comunicazione che non vengono "certificati" in alcun modo: basti pensare al caso in cui venga spedita una busta vuota. A parziale risoluzione del problema si usano talvolta fogli contenenti il messaggio e ripiegati a mo' di busta in modo tale che l'ufficio postale vi apponga il timbro con il datario. Questo genere di approccio, tuttavia, non impedisce che all'interno del primo "foglio-busta" possano essere inseriti altri fogli, questi – ovviamente – sprovvisti del timbro postale. Infine, l'ora di ricevimento di una raccomandata di tipo tradizionale non è garantita. Nemmeno la cosiddetta "ricevuta di ritorno" tradizionale, come stabilito anche da diverse sentenze di cassazione, offre garanzie.

La PEC è una soluzione che è stata introdotta solamente in Italia. Altri Paesi non hanno sentito l'esigenza di promuovere un meccanismo simile. Rispetto alla raccomandata A/R, la PEC offre sicuramente migliori garanzie perché basa il suo funzionamento su un sistema che coinvolge direttamente i provider Internet scelti rispettivamente da mittente e destinatario.

Prerequisito indispensabile per scambiarsi messaggi certificati, mediante l'uso della PEC, è

l'attivazione di un account presso un gestore (provider Internet) che fornisca questo tipo di servizio. Sono tanti i provider che oggi offrono caselle di posta elettronica compatibili PEC, alcuni molto economici.

I gestori certificati

Il *Centro Nazionale per l'Informatica nella Pubblica Amministrazione* (CNIPA) è l'organo preposto al controllo della posta elettronica certificata. E' infatti lo stesso CNIPA che si occupa di controllare le richieste di iscrizione avanzate dai provider interessati ad offrire, ai propri clienti, il servizio PEC e di redarre un elenco, pubblicamente accessibile, che riassume tutti i gestori accreditati. L'utente può scegliere, tra i provider indicati, quello preferito e richiedere, previa sottoscrizione di un contratto, una casella PEC. L'inserimento di un provider Internet nell'elenco delle società accreditate avviene in seguito ad un'istruttoria che valuta la bontà dei requisiti del gestore interessato a commercializzare il servizio PEC.

La PEC è nata in seno alla Pubblica Amministrazione, con lo scopo di sostituire l'impiego della raccomandata A/R tradizionale sia nelle comunicazioni tra enti che tra PA e cittadino. Di recente, per opera del CNIPA e di ISTI-CNR è stato avviato il processo di standardizzazione della PEC mediante una richiesta formale presentata all'IETF (*Internet Engineering Task Force*). La bozza presentata all'IETF, ente di standardizzazione caratterizzato da una struttura "aperta" formata da specialisti, tecnici e ricercatori, è consultabile facendo riferimento a questa pagina.

Come funziona la PEC

Il servizio PEC del provider al quale si è affidato il mittente del messaggio rilascia a quest'ultimo una ricevuta che costituisce la prova dell'avvenuta spedizione dell'e-mail. Tale comunicazione ha valore legale, data dalla legge stessa istitutiva della PEC, e conferma l'effettivo oppure il mancato invio della comunicazione.

Allo stesso modo, anche il gestore al quale si appoggia il destinatario dell'e-mail trasmette al mittente un messaggio attestante l'avvenuta consegna. Le varie ricevute contengono anche l'indicazione temporale per ciascuna operazione effettuata (ad esempio invio e consegna del messaggio).

Secondo quanto stabilito dalla normativa, i provider sono inoltre obbligati a tenere traccia delle comunicazioni trasmesse mediante PEC per un periodo di tempo pari a 30 mesi.

Per poter inviare una e-mail certificata mediante PEC è necessario che l'account che si impiega sia anch'esso PEC. Se si invia un'e-mail da un account di posta "non PEC" ad un account PEC il sistema che riceve il messaggio inviato solitamente genera un messaggio di errore (che prende il nome di "anomalia di trasporto") ma tale comportamento può dipendere dalla specifica configurazione software utilizzata dal provider. In alcuni casi, ad esempio, il mittente che utilizza un account di posta "non PEC" e tenta di trasmettere una comunicazione ad una casella PEC, può non ricevere alcun avviso.

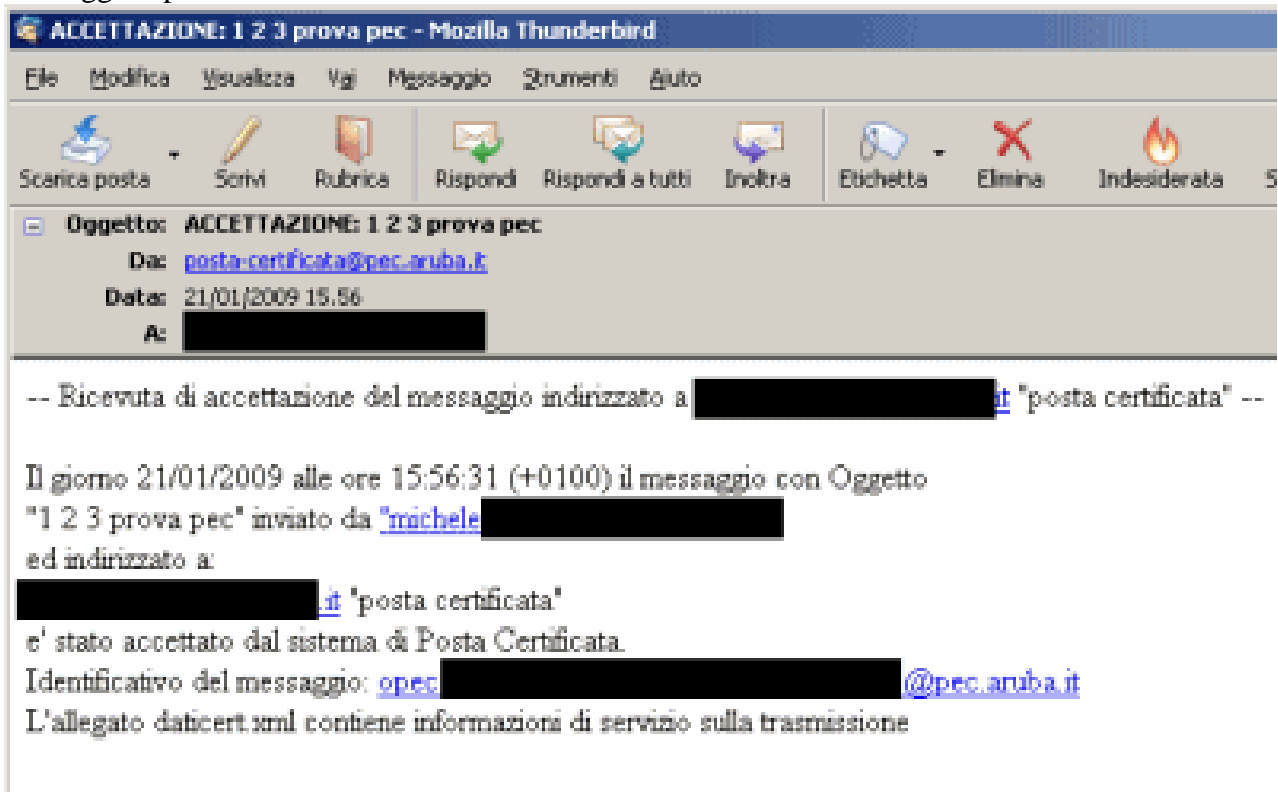
Alcuni aspetti critici legati all'uso della PEC che dovranno essere probabilmente affrontati sono anche i seguenti:

- al ricevimento di una raccomandata tradizionale, in caso di assenza del destinatario, allo stesso viene lasciato un avviso che attesta la giacenza della comunicazione presso l'ufficio postale di zona. Nel caso della PEC, quando il personal computer del destinatario è spento o non collegato ad Internet nessun avviso verrà notificato poiché resterà memorizzato (per quanto tempo?) sul server del provider Internet.
- qualora il personal computer del ricevente abbia un problema non verrà notificato nulla in

proposito a chi spedisce né tanto meno al server del provider per il quale la PEC sarà considerata come regolarmente recapitata.

- il titolare della casella PEC (es. un privato cittadino) è un ricevitore passivo di messaggi di posta elettronica equiparati ad una raccomandata A/R. I messaggi ricevuti possono potenzialmente essere di infinita natura (i.e. ingiunzioni di pagamento, atti di polizia giudiziaria, atti con scadenza onerosa,...). La loro ricezione e gestione con le modalità illustrate potrebbe causare qualche "mal di testa" al cittadino.

L'utilizzo della PEC è del tutto simile a quello della posta elettronica tradizionale. Per inviare e ricevere messaggi, infatti, è possibile ricorrere alla webmail messa a disposizione dal provider scelto e quindi accedervi attraverso il browser web oppure servirsi di un qualunque client di posta elettronica. Così come previsto dalla normativa, tuttavia, la comunicazione con i server del gestore Internet che offre il servizio PEC avviene utilizzando protocolli di comunicazione sicuri. Inoltre, come già anticipato, viene effettuata l'autenticazione di colui che opera dinanzi al personal computer - essendo impossibile autenticare il vero utente - sia in fase di invio che di ricezione dei messaggi di posta.



In figura, il server del provider Internet del mittente, che offre il servizio PEC, ha inviato una ricevuta che attesta la corretta presa in consegna della comunicazione.

CONSEGNA: 1 2 3 prova pec - Mozilla Thunderbird

File Modifica Visualizza Vai Messaggio Strumenti Aiuto

Scarica posta Scrivi Rubrica Rispondi Rispondi a tutti Inoltra Etichetta Elimina Indesiderata Stampa

Oggetto: CONSEGNA: 1 2 3 prova pec
 Da: posta-certificata@pec.aruba.it
 Data: 21/01/2009 15:56
 A: [REDACTED]

-- Ricevuta di avvenuta consegna del messaggio indirizzato a [REDACTED] <[\[REDACTED\]@pec.aruba.it](mailto:[REDACTED]@pec.aruba.it)> "posta certificata" --

Il giorno 21/01/2009 alle ore 15:56:32 (+0100) il messaggio con Oggetto "1 2 3 prova pec" inviato da "michele [REDACTED]" ed indirizzato a [REDACTED] <[\[REDACTED\]@pec.aruba.it](mailto:[REDACTED]@pec.aruba.it)> "posta certificata" e' stato correttamente consegnato al destinatario.
 Identificativo del messaggio: [REDACTED]@pec.aruba.it
 Il messaggio originale e' incluso in allegato, per aprirlo cliccare sul file "postacert.eml" (nella webmail o in alcuni oggetti del messaggio originale).
 L'allegato daticert.xml contiene informazioni di servizio sulla trasmissione

NOTA

La presenza o meno del messaggio originale, come allegato della ricevuta di consegna (file postacert.eml), dipende dal tipo di ricevuta di consegna che e' stato scelto di ricevere, secondo la seguente casistica:

- Ricevuta di consegna completa (Default): il messaggio originale completo e' allegato alla ricevuta di consegna.
- Ricevuta di consegna breve: il messaggio originale e' allegato alla ricevuta di consegna ma eventuali allegati presenti al suo interno verranno sostituiti con i rispettivi hash.
- Ricevuta di consegna sintetica: il messaggio originale non verra' allegato nella ricevuta di consegna.

Un'ulteriore ricevuta, spedita al mittente del messaggio, lo informa circa l'avvenuta consegna dell'e-mail certificata. In calce alla ricevuta è sempre riportato il messaggio originale.

Le valutazioni degli esperti

Il decreto legge 185/2008 contiene rilevanti modifiche al “Codice dell'Amministrazione Digitale” (D.Lgs. n.82/2005) ed al “Regolamento per l'utilizzo della Posta Elettronica Certificata” (D.P.R. n.68/2005). Come spiegano gli esperti, la nuova normativa contribuisce – ed è questo un fatto assolutamente positivo – ad accelerare i processi per l'abbandono del cartaceo, anche per quanto concerne l'invio di documentazione di particolare rilevanza.

Il punto sul quale si sono scatenate la maggiori critiche riguardava l'imposizione dell'utilizzo di uno strumento, qual è la PEC, a società e professionisti iscritti agli albi, oltre che alle pubbliche amministrazioni.

Come anticipato nell'introduzione, tuttavia, il decreto legge è stato successivamente modificato, in fase di conversione, con soddisfazione dell'associazione “Cittadini di Internet”, presieduta dall'Ing. Massimo Penco, che si era fatta promotrice di una denuncia resa alla UE.

All'utilizzo della PEC può essere sostituito, quindi, l'impiego di “*un analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali*”.

La soluzione alternativa sembra essere l'adozione di certificati S/MIME, interoperabili con qualunque sistema ed ormai disponibili, da anni, in ambito internazionale.

Secondo l'associazione “Cittadini di Internet”, la modifica apportata al decreto legge 185/2008 si allinea alla direttiva comunitaria, permette di liberalizzare il mercato e pone soluzione al problema dell'ipotizzato utilizzo esclusivo della PEC, di matrice solamente italiana.

La soluzione alternativa alla PEC: i certificati S/MIME

Tutti i programmi (client) per l'invio e la ricezione della posta elettronica che supportano il formato S/MIME sono in grado di gestire certificati digitali: questi ultimi servono a firmare sia le e-mail che i relativi allegati rendendoli immodificabili e dando valore legale agli stessi. In aggiunta, è anche possibile crittografare i messaggi rendendo così sicuro il loro trasporto.

MIME è l'acronimo di *Multipurpose Internet Mail Extensions* e fissa uno standard per il formato di un messaggio di posta elettronica. Ogni messaggio inviato attraverso un server SMTP è considerabile come in formato MIME. Le varie parti di un'e-mail ed, in particolare, le indicazioni MIME inserite al suo interno, specificano, ad esempio, il formato con cui viene inviato il messaggio (solo testo o html), la codifica utilizzata, eventuali allegati e così via.

S/MIME (*Secure Multipurpose Internet Mail Extensions*) è uno standard per la crittografia a chiave pubblica e per la firma dei messaggi di posta elettronica che si inserisce all'interno delle specifiche di MIME. S/MIME, originariamente sviluppato da RSA Security, fornisce la possibilità di autenticare, verificare l'integrità, garantire il non ripudio (utilizzando la firma digitale) e proteggere il messaggio (utilizzando la crittografia) trasmesso in Rete.

Rispetto alla PEC, l'impiego di un certificato S/MIME permette ad esempio di certificare l'intero contenuto del messaggio che si invia, consente di inviare comunicazioni a qualunque tipo di indirizzo e-mail, è interoperabile con qualunque sistema ed è valido in tutto il mondo. Inoltre, l'uso di un certificato S/MIME consente di fidare su di una soluzione che garantisce massima portabilità ed in più è in grado di permettere la protezione del contenuto del messaggio grazie alla crittografia.

Due esempi di società (“Certification Authority” o CA) che mettono a disposizione, gratuitamente se per uso personale, certificati digitali da utilizzare per la posta elettronica sono Globaltrust (italiano) e Thawte.

La “Certification Authority” è un ente (*trusted third party*), pubblico o privato, che è abilitato al rilascio di un certificato digitale previa verifica delle generalità dell'utente richiedente. Il sistema adottato è quello “a chiave pubblica” (o “asimmetrica”): una chiave viene inserita all'interno del certificato (“pubblica”) mentre l'altra, collegata alla chiave pubblica, deve restare assolutamente segreta e conservata con cura da parte dell'utente (“chiave privata”).

La coppia chiave pubblica-chiave privata può essere generata autonomamente da parte dell'utente servendosi di un programma “ad hoc” (ad esempio, GnuPG; ved., in proposito, questo articolo). Le CA rappresentano la soluzione tra la chiave pubblica e la persona che è in possesso della relativa chiave privata.

Senza passare per una CA, due interlocutori possono creare la propria coppia chiave privata/pubblica, pubblicando poi quelle pubbliche su un “keyserver” (si tratta di server, di libero

accesso, che raccolgono le chiavi pubbliche di milioni di utenti di tutto il mondo).

Nella letteratura, quando si parla di crittografia, ci si imbatte spessissimo nei due amici Alice e Bob. Si tratta di nomi convenzionali che vengono solitamente utilizzati per riferirsi a due interlocutori. Quando altre due persone si aggiungono alla comunicazione, vengono generalmente usati i nomi di Carol e Dave. Non può mancare “il cattivo”, di solito identificato con il nome di Mallory.

Supponiamo che Bob voglia inviare un messaggio ad Alice, firmato e crittografato. Egli provvede a firmarlo usando la sua chiave privata quindi lo codifica usando la chiave pubblica di Alice, recuperata – ad esempio – da un “keyserver”, pubblicata sul sito web di Alice o comunicata precedentemente via e-mail. Una volta che Alice riceve la comunicazione, questa viene decifrata usando la sua chiave privata verificando la firma del messaggio usando la chiave pubblica di Bob. Alice, a questo punto, sa che il messaggio era a lei destinato e che è stato firmato da Bob. Purtroppo, non c'è la piena certezza che la chiave usata sia realmente di proprietà di Bob perché manca un'attestazione “ufficiale” circa la corrispondenza tra la chiave e la persona “fisica”. Il “malintenzionato” Mallory potrebbe essere in grado di sostituire la chiave pubblica del destinatario con una “fasulla” in modo tale da poter intercettare tutte le comunicazioni.

Le CA si occupano di controllare l'identità di un utente producendo, dopo le necessarie verifiche, un certificato che è firmato digitalmente dalla CA stessa (che gode della fiducia delle parti coinvolte nella comunicazione). Grazie a questo espediente, è possibile stabilire immediatamente l'attendibilità e la validità di qualunque certificato digitale.

Utilizzo dei certificati S/MIME nella pratica

Chiarito il ruolo e l'importanza delle CA, vediamo come sia possibile, nella pratica, sfruttare un certificato S/MIME per l'invio di qualunque genere di messaggio di posta elettronica.

A titolo esemplificativo, utilizziamo il certificato che Globaltrust mette a disposizione di tutti i richiedenti, per scopi personali. Il certificato rilasciato dalla CA italiana, è completamente gratuito ed ha validità annuale, con la possibilità di effettuare ulteriori rinnovi sempre a titolo non oneroso.

Per richiedere a GlobalTrust il proprio certificato digitale è sufficiente visitare questa pagina web, inserire i propri dati anagrafici ed una password adeguatamente complessa.

Entro pochi giorni si riceverà così un'e-mail all'indirizzo di posta elettronica specificato all'atto della richiesta del certificato: il messaggio contiene un link da seguire per provvedere all'installazione automatica del certificato personale sul proprio sistema. La procedura di richiesta ed attivazione del certificato digitale va effettuata utilizzando il medesimo browser web.

Il certificato personale così richiesto consentirà di codificare e firmare digitalmente i propri messaggi di posta elettronica garantendo riservatezza, confidenzialità, autenticità, integrità e non ripudio delle comunicazioni trasmesse.

GlobalTrust (o comunque la CA che emette il certificato) provvede a fornire all'utente facente richiesta, un certificato contenente l'identificativo dell'algoritmo crittografico usato, un numero di serie, la firma digitale, il nome della CA, le informazioni riguardanti la validità ed una chiave pubblica. Questo insieme di informazioni identifica colui che ha richiesto il certificato come unico possessore ed utilizzatore dello stesso.

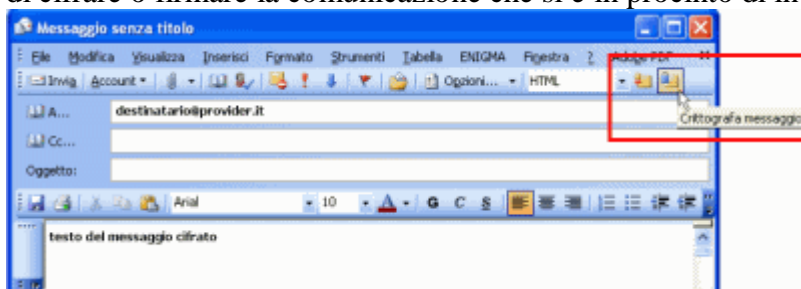
Una volta attivato e scaricato il certificato S/MIME, questo potrà essere salvato su disco fisso in modo da essere facilmente impiegato, per esempio, con un qualsiasi client di posta elettronica. Il certificato potrà essere salvato sotto forma di file con estensione .pfx: tale file non dovrà essere trasmesso a terzi dato che contiene anche la propria chiave privata.

Nel caso si sia importato il certificato in Internet Explorer, questo potrà essere salvato su disco in

formato .pfx avviando il browser Microsoft, cliccando sul menù *Strumenti, Opzioni Internet* quindi su *Contenuto*. Facendo riferimento al pulsante *Certificati* quindi selezionando il proprio certificato S/MIME dalla scheda *Personale* ed infine premendo *Esporta...*, si potrà produrre il file .pfx. In tutte le fasi di esportazione ed importazione del certificato S/MIME verrà sempre richiesta la password scelta a protezione del file: mai dimenticarla.

Per impostare Outlook affinché utilizzi il certificato personale, basta far riferimento al menù *Strumenti, Opzioni* del programma quindi alla scheda *Protezione*. Cliccando su *Impostazioni* ci si può assicurare che il certificato in uso sia quello ricevuto da GlobalTrust ed eventualmente importarlo in modo manuale.

I pulsanti *Codifica* e *Firma* visualizzati in fase di composizione di un'e-mail permetteranno quindi di cifrare o firmare la comunicazione che si è in procinto di inviare.



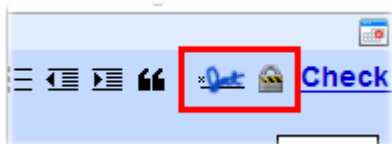
Con Outlook, una volta ricevuto ed aperto il messaggio, il certificato verrà automaticamente installato sul sistema del destinatario.

Per aggiungere la chiave pubblica di un destinatario alla lista dei certificati, è sufficiente cliccare sul simbolo raffigurante una coccarda di colore rosso (contenuto nell'e-mail ricevuta dall'interlocutore) quindi cliccare sulla voce *Aggiungi ai contatti di Outlook*.

La chiave pubblica del contatto verrà così automaticamente associata al contatto stesso e risulterà visibile selezionando la scheda *Certificati*.

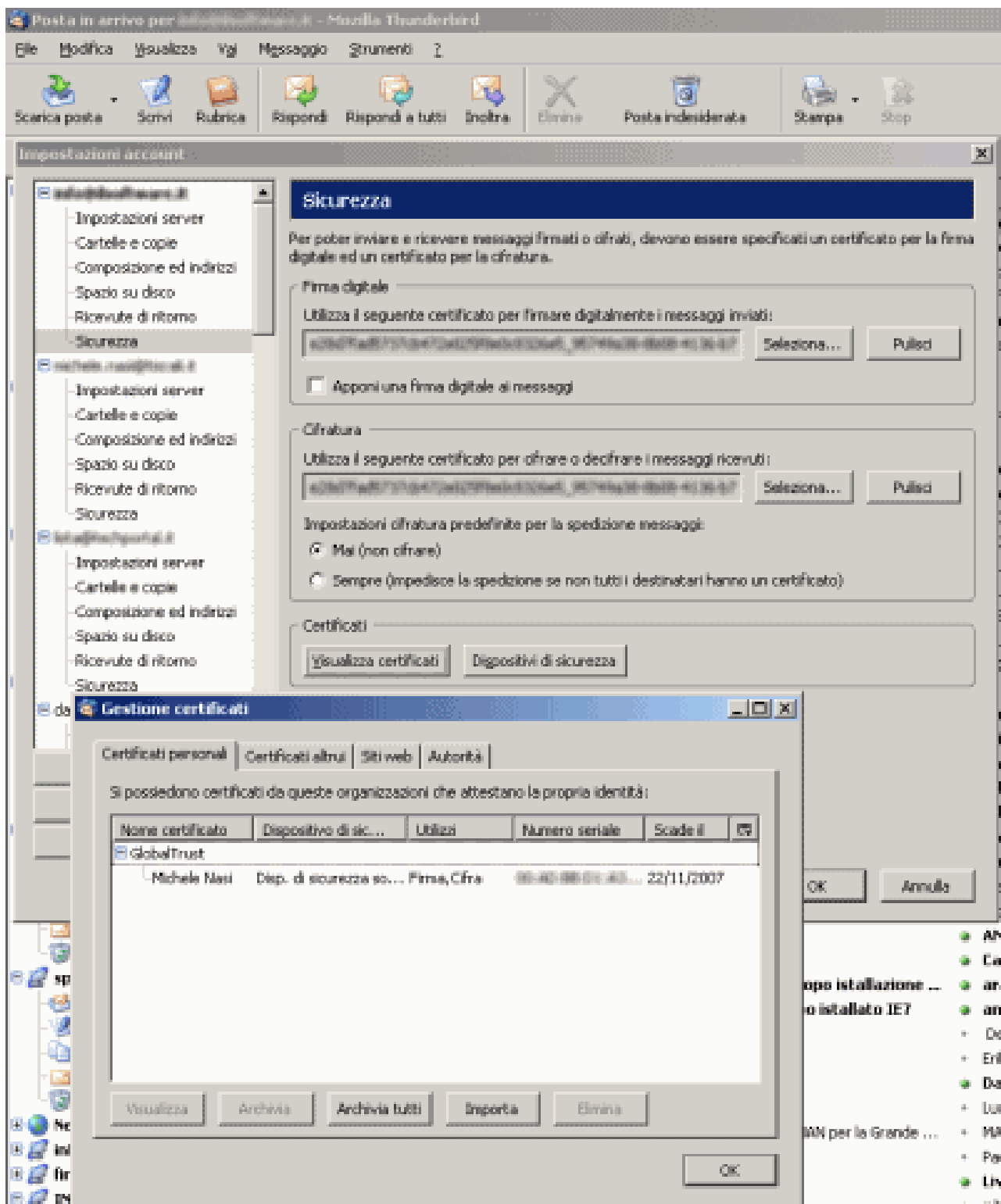
Se il certificato dell'interlocutore si presenta sotto forma di allegato (estensione .cer) al messaggio di posta elettronica, sarà possibile aggiungerlo alla lista selezionando il comando *Importa*.

Il certificato personale ottenibile facendo richiesta a Globaltrust così come a qualunque CA riconosciuta, è ovviamente utilizzabile anche con altri client di posta elettronica. Nel caso di Mozilla Thunderbird, ad esempio, diventa possibile cifrare e firmare messaggi senza ricorrere ad estensioni sviluppate da terzi (la più famosa è la open source Enigmail; ved. questo nostro articolo, in proposito) e potendo fidare sulla certificazione resa da Globaltrust.



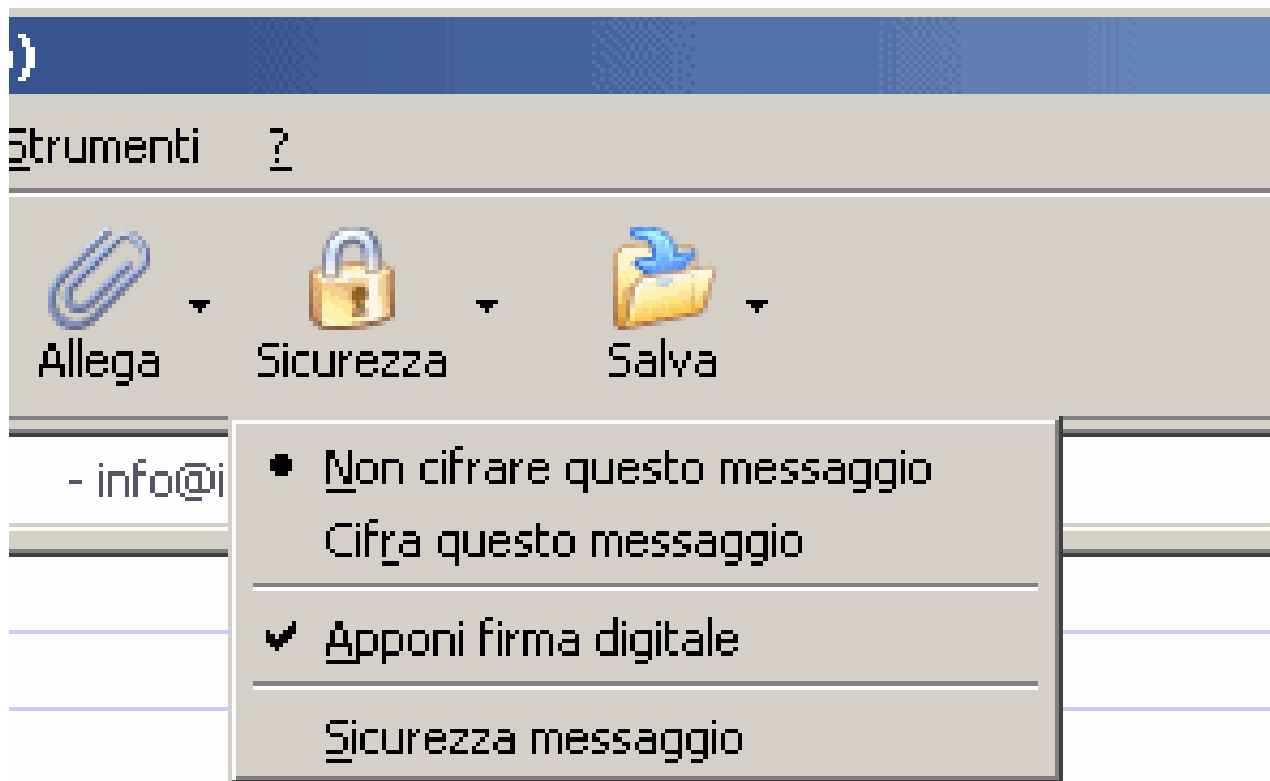
La gestione dei certificati in Mozilla Thunderbird si effettua cliccando su *Strumenti, Impostazioni account* quindi sulla voce *Sicurezza*.

Cliccando su *Visualizza certificati* è possibile importare certificati e controllare quelli disponibili. Selezionando la scheda *Certificati personali* quindi servendosi del pulsante *Importa*, si può aggiungere in elenco il certificato (in formato .pfx) ottenuto gratuitamente, ad esempio, da Globaltrust.



Nella scheda *Certificati altrui*, invece, Mozilla Thunderbird aggiunge automaticamente i certificati, allegati ai vari messaggi di posta elettronica, ricevuti da parte dei propri interlocutori.

Dopo aver importato il proprio certificato, è sufficiente fare clic sui pulsanti *Seleziona* presenti nei riquadri *Utilizza il seguente certificato per firmare digitalmente i messaggi* ed *Utilizza il seguente certificato per cifrare o decifrare i messaggi ricevuti* per indicare a Thunderbird che si intende farne uso.



In fase di composizione di un messaggio, si dovrà far riferimento al pulsante *Sicurezza* quindi alle voci *Cifra questo messaggio* ed *Apponi firma digitale*.

Nel caso di Mozilla Thunderbird, anziché una coccarda rossa, all'interno della finestra che visualizza il contenuto di un messaggio firmato digitalmente, verrà aggiunta - in alto a destra - un'icona raffigurante una penna.

Per chi utilizzasse il servizio Google Gmail da web, senza quindi appoggiarsi ad un client di posta, è possibile inviare e-mail firmate digitalmente e cifrate ricorrendo all'add-on gratuito per Mozilla Firefox denominato *Gmail S/MIME* e scaricabile da questa pagina. Dopo aver installato l'add-on, la finestra di composizione di un messaggio di Gmail risulterà arricchita di due nuovi pulsanti: l'uno permette di firmare l'e-mail, l'altro di cifrarne il contenuto.

Ricordiamo comunque che il servizio di posta Gmail messo a disposizione da Google è gestibile con qualunque client e-mail in modo da dover evitare di accedere via web alla propria casella di posta elettronica (le istruzioni per la configurazione del proprio software preferito per la gestione dei messaggi di posta sono consultabili facendo riferimento a questa pagina).

Per usare il certificato S/MIME offerto da Globaltrust nella versione web di Google Gmail, si dovrà ovviamente importarlo in Mozilla Firefox accedendo al menù *Strumenti, Opzioni*, cliccando sulla scheda *Avanzate* quindi su *Cifratura* ed infine sul pulsante *Mostra certificati*. Dalla scheda *Certificati personali*, si dovrà cliccare su *Importa...* e selezionare il file .pfx relativo al proprio certificato S/MIME.

L'utilizzo della **firma digitale** consente di fidare su **autenticazione, integrità e non ripudio** mentre la **codifica del messaggio** permette di aggiungere le caratteristiche di **riservatezza e confidenzialità** (tutte queste peculiarità sono intrinseche nell'utilizzo di un **certificato S/MIME**).