

► Obblighi per professionisti

PEC, i tuoi messaggi e-mail sotto controllo

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 apportate numerose modifiche alla versione iniziale dello stesso. Nella sostanza, l'intervento sembra aver rimosso l'obbligatorietà della PEC che è uno standard

Addio raccomandate cartacee. Con la Posta Elettronica Certificata le comunicazioni "ufficiali" viaggiano su Internet.

I passi necessari per creare un certificato digitale, divenuto obbligatorio dopo la conversione del decreto legge

di matrice italiana. L'impresa o 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" (si veda a proposito la Legge 28 gennaio n.2, art. 16 comma 6).

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

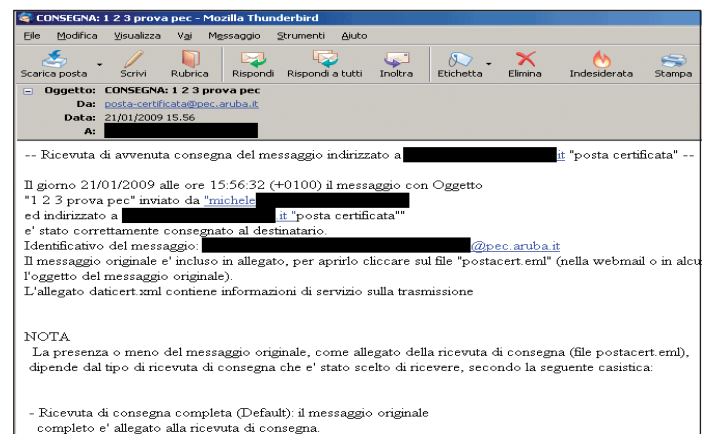
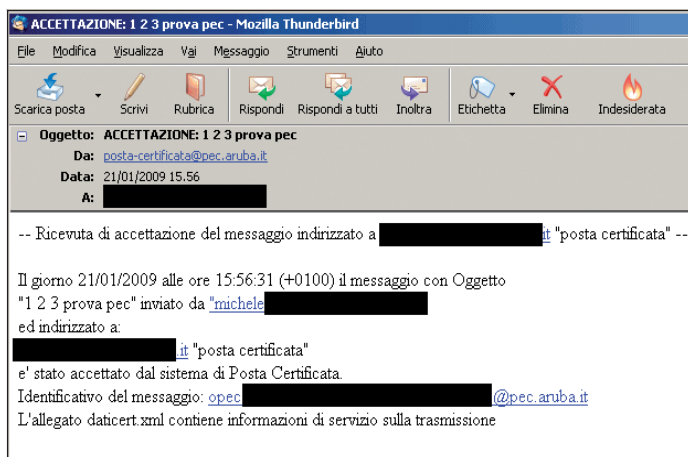
posta di tipo tradizionale ormai da diversi anni. Come anticipato, la PEC (si veda anche l'articolo a pag. 98) è stata ideata con l'intento di attribuire al messaggio di posta elettronica lo stesso valore di una raccomandata con ricevuta di ritorno di tipo tradizionale. Rispetto alla raccomandata A/R, 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 infatti l'attivazione di un account presso un gestore (provider Internet) che fornisca questo tipo di servizio.

I gestori certificati

Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) è l'organo preposto al controllo della posta elettronica certificata. È 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 ([www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Posta_Elettronica_Certificata_\(PEC\)/Elenco_pubblico_dei_gestori/](http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Posta_Elettronica_Certificata_(PEC)/Elenco_pubblico_dei_gestori/)), 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.

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 standardizzazio-



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

Il mittente del messaggio di posta elettronica certificata ottiene una ricevuta che attesta l'avvenuta consegna dell'e-mail precedentemente spedita a un account PEC. In calce alla ricevuta è sempre riportato il messaggio originale

ne caratterizzato da una struttura "aperta" formata da specialisti, tecnici e ricercatori, è consultabile facendo riferimento alla pagina raggiungibile all'indirizzo <http://tools.ietf.org/html/draft-gennai-smime-cni-pa-pec-02>.

Come funziona la posta elettronica certificata

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, dato 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.

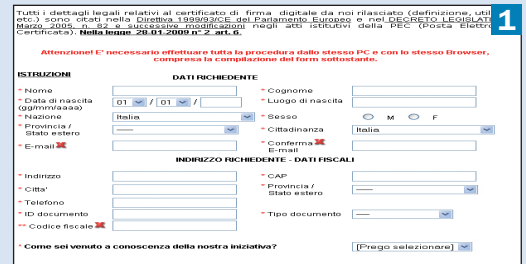
Per poter inviare una e-mail certificata mediante PEC è necessario che l'account che si impiega sia anch'esso PEC. Se si invia un'e-mail da un account di posta "non PEC" ad un account PEC il sistema che riceve il messaggio inviato solitamente genera un messaggio di errore (che prende il nome di "anomalia 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.

L'utilizzo della PEC è del tutto simile a quello della posta elettronica tradizionale. Per inviare e ricevere messaggi, infatti, è possibile ricorrere alla web-mail messa a disposizione dal provider scelto e quindi accedervi attraverso il browser 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 uti-

Come richiedere il certificato digitale con GlobalTrust

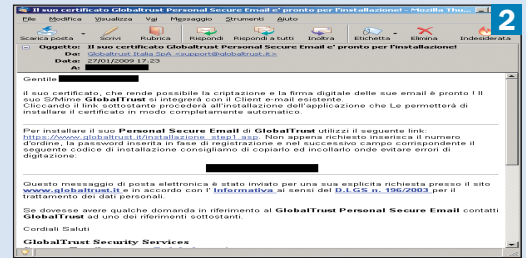
► Registrazione

Per richiedere a GlobalTrust il proprio certificato digitale S/MIME è sufficiente andare alla pagina https://www.globaltrust.it/modulo_reg_smime.asp e inserire i propri dati anagrafici. Dopodiché bisogna scegliere una password particolarmente articolata.



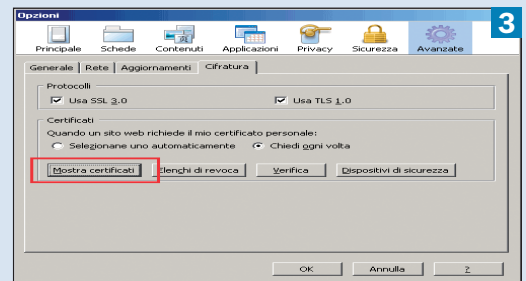
► Certificato S/MIME

Una volta che il certificato S/MIME è stato generato ed è pronto per l'utilizzo da parte dell'utente, la CA informa circa la sua disponibilità attraverso una comunicazione trasmessa via e-mail. Seguendo le indicazioni riportate nel messaggio, sarà possibile scaricare ed installare il proprio certificato. Nel caso di Globaltrust, la procedura di download ed installazione del certificato sarà avviabile sia da Microsoft Internet Explorer che da Mozilla Firefox.



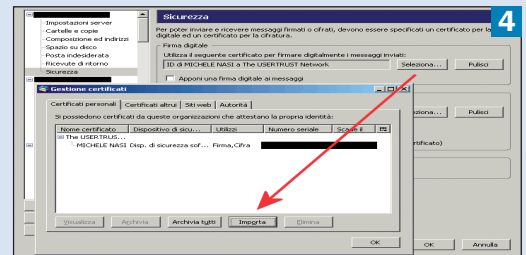
► Installazione del certificato

Effettuando l'installazione del certificato con Firefox, questo sarà inserito nell'apposita scheda del browser accessibile cliccando su *Strumenti, Opzioni*, selezionando la scheda *Avanzate* quindi *Cifratura* ed infine il pulsante *Mostra certificati*.



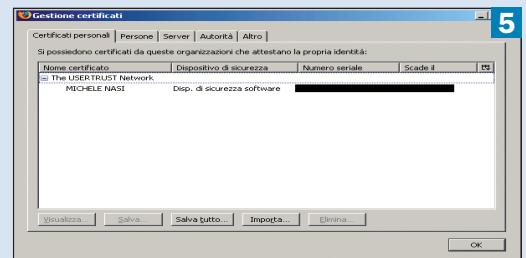
► Esportazione del certificato

Il certificato S/MIME è esportabile, da Firefox, cliccando sul pulsante *Salva*. Una volta specificato il nome da attribuire, si otterrà un file con estensione .p12. Tale file potrà essere importato in qualunque client di posta, ad esempio in Mozilla Thunderbird usando il comando *Importa*.



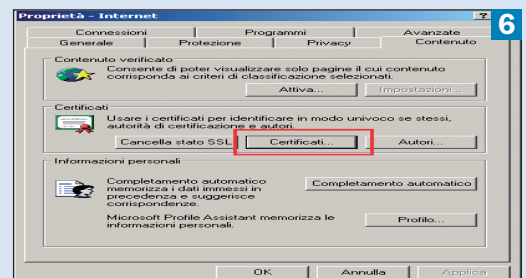
► Visualizzazione in Firefox

All'interno della scheda *Certificati personali* di Firefox, si troverà il proprio certificato S/MIME, appena aggiunto. Un doppio clic permette di rilevare tutti i dettagli relativi al proprio certificato digitale.



► Visualizzazione in Internet Explorer

Nel caso di Internet Explorer, per visualizzare il certificato S/MIME installato, è possibile accedere al *Pannello di controllo* di Windows, fare doppio clic su *Opzioni Internet*, cliccare sulla scheda *Contenuto* quindi sul pulsante *Certificati*: all'interno della scheda *Personale* si troverà il proprio certificato S/MIME.



lizzando protocolli di comunicazione sicuri. Inoltre, come già anticipato, viene effettuata l'autenticazione di colui che opera dinanzi al PC, essendo impossibile autenticare il vero utente sia in fase di invio che di ricezione dei messaggi di posta.

Le soluzioni alternative

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 immutabili e dando valore legale agli stessi. In aggiunta, è anche possibile crittografare i messaggi rendendo così sicuro il loro trasporto.

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 digitale S/MIME garantisce massima portabilità ed in più è in grado di permettere la protezione del contenuto del messaggio grazie alla crittografia.

Il certificato digitale viene messo a disposizione dalle cosiddette *Certification Authority* (CA), società appunto preposte al rilascio di questi certificati previa verifica delle generalità dell'utente richiedente. In Italia, si segnalano ad esempio GlobalTrust o Thawte che mettono a disposizione, gratuitamente se per uso personale, certificati digitali da utilizzare per la posta elettronica. L'operazione può essere effettuata via Internet: è indispensabile inserire tutti i dati richiesti che comprendono

no, tra l'altro, il riferimento ad un documento di identità (carta d'identità, patente di guida, passaporto). Il richiedente deve anche scegliere una password adeguatamente complessa che sarà impiegata per la gestione del certificato S/MIME.

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).

Le CA in questo processo rappresentano la soluzione tra la chiave pubblica e la persona che è in possesso della relativa chiave privata. Di fatto, 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.

La coppia chiave pubblica-chiave privata può essere generata autonomamente da parte dell'utente servendosi di un programma ad hoc (ad esempio, GnuPG).

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).

Utilizzo dei certificati S/MIME nella pratica

Chiarito il ruolo e l'importan-

Le chiavi pubbliche e private

Nella letteratura, quando si parla di crittografia, ci si imbatte molto spesso 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.

za 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 la pagina Web www.globaltrust.it/modulo_reg_smime.asp, 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.

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 menu *Strumenti, Opzioni Internet* quindi su *Contenuto*. Facendo riferimento al pulsante *Certificati* quindi selezionando il proprio certificato S/MIME

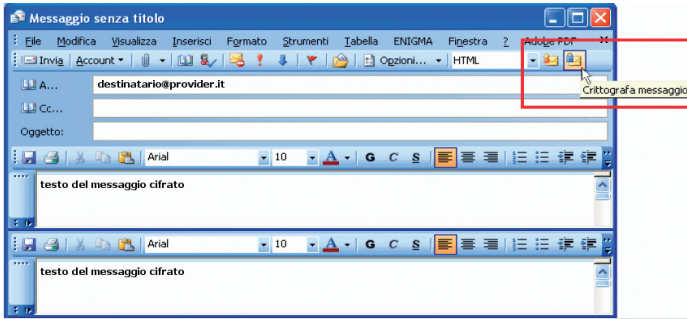
Firmare e crittografare la posta con Gmail

Chi utilizza il servizio Google Gmail da Internet, senza quindi appoggiarsi ad un client di posta, può inviare e-mail firmate digitalmente e cifrate ricorrendo all'add-on gratuito per Mozilla Firefox denominato Gmail S/MIME e scaricabile dalla pagina seguente: <https://addons.mozilla.org/it/firefox/addon/592>.

Dopo aver installato l'add-on, la finestra di composizione di un messaggio di Gmail risulterà arricchita di due nuovi pulsanti: uno permette di firmare l'e-mail, l'altro di cifrare il contenuto. Per usare il certificato S/MIME offerto da Globaltrust nella versione Web di Google Gmail, si dovrà ovviamente importarlo in Mozilla Firefox accedendo al menu *Strumenti, Opzioni*, cliccando sulla scheda *Avanzate* quindi su *Cifatura* 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.



Una volta installata l'estensione Gmail S/MIME, l'interfaccia Web del servizio di posta elettronica di Google si arricchirà di due nuovi pulsanti: il primo permetterà di firmare digitalmente il messaggio, il secondo di cifrare il contenuto



Outlook permette di cifrare e firmare qualunque messaggio di posta utilizzando il certificato S/MIME personale presente nella finestra Opzioni Internet, Contenuto, Certificati del Pannello di controllo di Windows

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.

Il certificato digitale con Outlook e Thunderbird

Per impostare Outlook affinché utilizzi il certificato personale, basta far riferimento al menu *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) e potendo contare 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. 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).

Michele Nasi

Glossario

PEC. Acronimo di *Posta Elettronica Certificata*. 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. 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. Rispetto alla raccomandata A/R, la PEC offre migliori garanzie perché basa il suo funzionamento su un sistema che coinvolge direttamente i provider Internet qualificati, il cui elenco è disponibile sul sito del CNIPA.

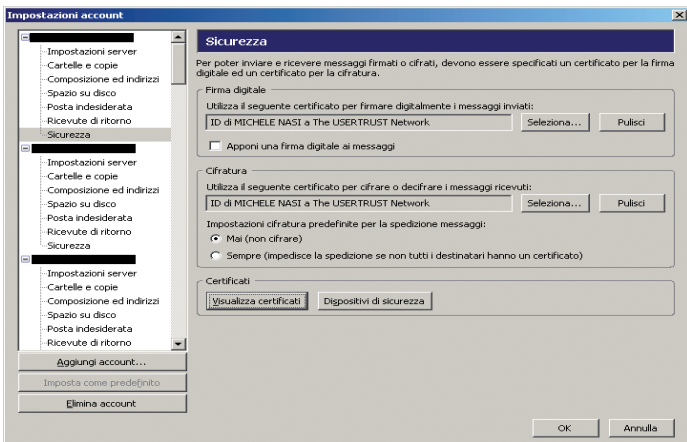
MIME. È l'acronimo di *Multipurpose Internet Mail Extensions* e fissa uno standard per il formato di un messaggio di posta elettronica. Ogni messaggio inviato attraverso un server SMTP è considerabile come in formato MIME. Le varie parti di un'e-mail ed, in particolare, le indicazioni MIME inserite al 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.

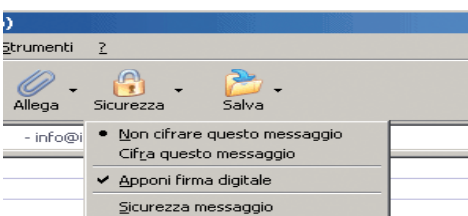
S/MIME. Secure Multipurpose Internet Mail Extensions, standard per la crittografia a chiave pubblica e per la firma dei messaggi di posta elettronica che si inserisce all'interno delle specifiche di MIME. S/MIME, originariamente sviluppato da RSA Security, fornisce la possibilità di autenticare, verificare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

Certification Authority. È un ente (trusted third party), pubblico o privato, è abilitato al rilascio di un certificato digitale previa verifica delle generalità dell'utente richiedente.

Keyserver. Si tratta di server, di libero accesso, che raccolgono le chiavi pubbliche di milioni di utenti di tutto il mondo.



Nella finestra delle impostazioni degli account di posta è possibile, con Thunderbird, indicare quale certificato S/MIME debba essere eventualmente impiegato per firmare e/o per cifrare la posta. Attraverso i pulsanti *Seleziona*, si può importare il proprio certificato S/MIME, precedentemente esportato da Firefox o da Internet Explorer



In fase di composizione di un messaggio, Thunderbird mostra - nella barra degli strumenti - i comandi che permettono di firmare l'e-mail (Apponi firma digitale) oppure crittografarne il contenuto