

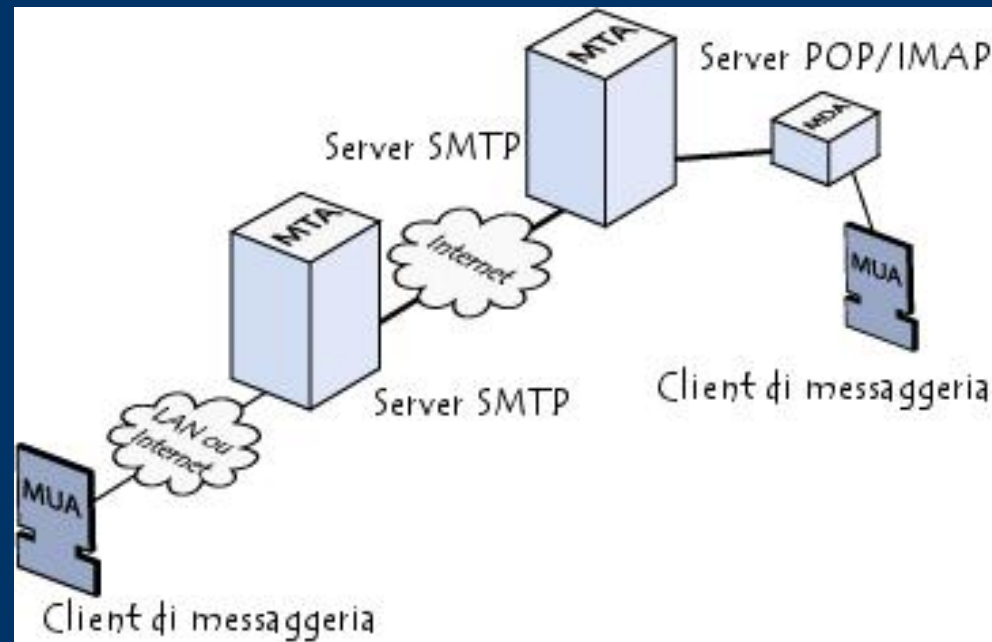
Internet:

*conoscerlo al meglio
per usarlo meglio*

La Posta elettronica

- E-mail client
- Lettura email via POP
- Lettura email via IMAP
- Lettura e-mail via web
- Proteggersi dal phishing (furto d'identità)
- E-mail con firma digitale
- Posta elettronica certificata
- Antivirus

Funzionamento posta elettronica



Al momento dell'invio di un'email, il messaggio è inoltrato da server in server fino al server di messaggia del destinatario. Più esattamente, il messaggio è inviato al server di posta elettronica incaricato del trasporto (detto MTA per Mail Transport Agent), fino all'MTA del destinatario.

Funzionamento posta elettronica

Su internet, gli MTA comunicano fra loro grazie al protocollo SMTP e sono logicamente chiamati server SMTP (talvolta server di posta in uscita).

Il server MTA del destinatario consegna quindi la posta al server di posta elettronica in entrata (detto MDA per Mail Delivery Agent), che immagazzina il messaggio in attesa che l'utente venga a rilevarlo.

Il ritiro della posta avviene tramite un software detto MUA (Mail User Agent).

Quando il MUA è un software installato sul sistema dell'utente, si parla di e-mail client (ad esempio Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail o Lotus Notes).

Quando si tratta di un'interfaccia web che permette di interfacciarsi al server di posta in entrata, si parla allora di webmail.

E-mail client (*client di posta elettronica*)

Un client di posta (o Mail User Agent, MUA) è un programma che consente di gestire la composizione, la trasmissione, la ricezione e l'organizzazione di e-mail (messaggi di posta elettronica) da e verso un server di posta.

Il termine "client" viene utilizzato perché il servizio di posta elettronica si basa su un'architettura client-server. Il client si occupa della composizione e della lettura, il server si occupa della trasmissione dei messaggi.

Esiste una particolare categoria di client e-mail definita "client webmail". Si tratta di particolari programmi eseguiti da siti web che permettono di gestire i propri messaggi da qualsiasi postazione: da casa, dall'ufficio, in un Netcafé, ecc.

Letture e-mail via POP

Il Post Office Protocol (detto anche POP) è un protocollo che ha il compito di permettere, mediante autenticazione, l'accesso ad un account di posta elettronica presente su di un host per scaricare le e-mail del relativo account. Il pop (nella versione 3) rimane in attesa sulla porta 110 dell'host (di default, ma può anche essere diversa) per una connessione TCP da parte di un client. I messaggi di posta elettronica, per essere letti, devono essere scaricati sul computer (questa è una notevole differenza rispetto all'IMAP), anche se è possibile lasciarne una copia sull'host. Il protocollo POP3 non prevede alcun tipo di cifratura, quindi le password utilizzate per l'autenticazione fra server e client passano in chiaro.

Letture e-mail via IMAP

L'Internet Message Access Protocol (IMAP), a volte anche chiamato Interactive Mail Access Protocol, è un protocollo di comunicazione per la ricezione di e-mail. Il significato "Interactive Mail Access Protocol" è stato valido fino alla versione 3, dalla quarta in poi è cambiato in "Internet Message Access Protocol".

La porta predefinita sull'host è la 143. Se si utilizza una connessione sicura tramite SSL, allora la porta è la 993.

Differenze tra IMAP e POP

L'IMAP è principalmente utilizzato nelle grandi network come università o aziende, dove un utente cambia postazione spesso: con il POP3, sarebbe necessario scaricare i messaggi ogni volta che si cambia pc, mentre con l'IMAP si possono scaricare solo i nuovi messaggi o accedere ad un messaggio specifico senza dover scaricare gli altri. Ecco un elenco delle caratteristiche dell'IMAP ma non del POP:

- **Accesso alla posta sia online che off-line**
- **Più utenti possono utilizzare la stessa casella di posta**
- **Supporto all'accesso a singole parti di un messaggio**
- **Supporto per attributi dei messaggi tenuti dal server**
- **Possibilità di fare ricerche sul server**

Letture e-mail via web

Una Webmail è un'applicazione web che permette di gestire uno o più account di posta elettronica attraverso un navigatore web.

Generalmente viene fornita come servizio ad abbonati di un provider di connessione internet oppure come servizio di posta elettronica.

In alcune aziende la webmail viene fornita come servizio ai dipendenti in modo che possano leggere la propria posta da casa oppure fuori sede.

Attraverso l'interfaccia grafica si stabilisce una normale connessione verso un server di posta, generalmente si utilizza IMAP.

Letture e-mail via web

Vantaggi:

- **Possibilità di leggere la propria posta ovunque vi sia una connessione ad internet**
- **I messaggi non necessitano di essere scaricati**
- **I servizi gratuiti permettono registrazioni anonime**
- **Le caselle di posta possono essere amministrate molto facilmente**

Letture e-mail via web

Svantaggi:

- **È richiesta una connessione sia per la visualizzazione che per la composizione dei messaggi.**
- **Una connessione lenta inficia la funzionalità generale della webmail.**
- **Le funzionalità di composizione di messaggi sono generalmente limitate sia per la formattazione sia per la dimensione totale di un messaggio**

▣ **Phishing** (*furto d'identità*)

In ambito informatico il phishing ("spillaggio di dati sensibili", in italiano) è una attività illegale che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto d'identità mediante messaggi di posta elettronica fasulli. Grazie a messaggi che imitano grafico e logo dei siti istituzionali, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc..

☰ **Proteggersi dal phishing** (furto d'identità)

La maggior parte delle e-mail fraudolente, presentano, di solito, le seguenti caratteristiche:

- non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali, per motivi non sempre ben specificati (es.: scadenza, smarrimento, problemi tecnici, ecc.)
- anche in presenza di una personalizzazione, l'e-mail non fa quasi mai riferimento al nome e cognome del destinatario ma a un indirizzo di posta elettronica
- fanno uso di toni "intimidatori" (es.: minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente)
- non riportano una data di scadenza per l'invio delle informazioni
- contengono errori di ortografia e sono spesso scritte in una forma poco corretta
- chiedono di non rispondere al mittente ma di cliccare sull'indirizzo fornito

Firma digitale in e-mail

La firma digitale è un metodo per attestare che l'e-mail ricevuta sia stata effettivamente inviata dal mittente e che il contenuto non sia stato alterato, dato che ogni minima modifica comprometterebbe la validità della firma.

Essa viene rilasciata da appositi certificatori, di solito a pagamento.

Quando si firma digitalmente un messaggio, si aggiungono una firma digitale e una chiave pubblica.

I destinatari possono utilizzare la firma digitale per verificare l'identità del mittente.

Possono inoltre utilizzare la chiave pubblica del mittente per inviare posta crittografata che soltanto il mittente può leggere mediante la chiave privata.

Per inviare messaggi crittografati, è necessario che la Rubrica contenga gli ID digitali dei destinatari.

In tal modo si potranno codificare i messaggi utilizzando le chiavi pubbliche dei destinatari. Quando un destinatario riceve un messaggio crittografato utilizza la chiave privata per decodificarlo e leggerlo.

Prima di iniziare a inviare messaggi firmati digitalmente è necessario avere un ID digitale e impostare il proprio account di posta elettronica per utilizzarlo. Se si inviano messaggi crittografati, è necessario che la Rubrica contenga un ID digitale per ciascun destinatario.

Come richiedere un certificato di firma digitale in modo gratuito

https://www.globaltrust.it/modulo_reg_smime.asp

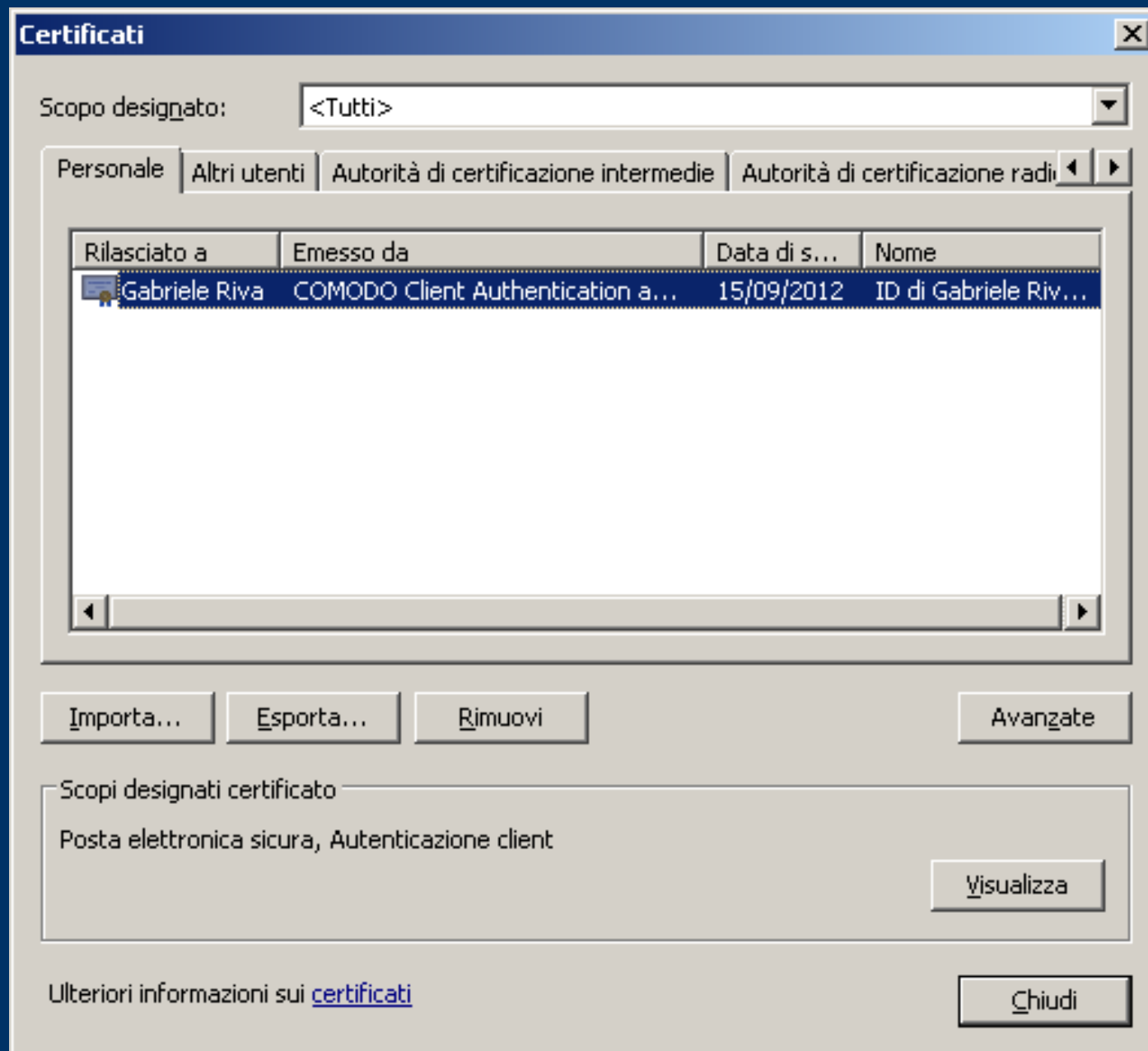
- Compilare il modulo
- Entro 24/48 ore verrà spedita un'e-mail con le istruzioni per scaricare il certificato.

Il certificato verrà installato nel sistema tramite il browser.

Per poter utilizzare il certificato con Thunderbird esso andrà esportato e reimportato in Thunderbird.

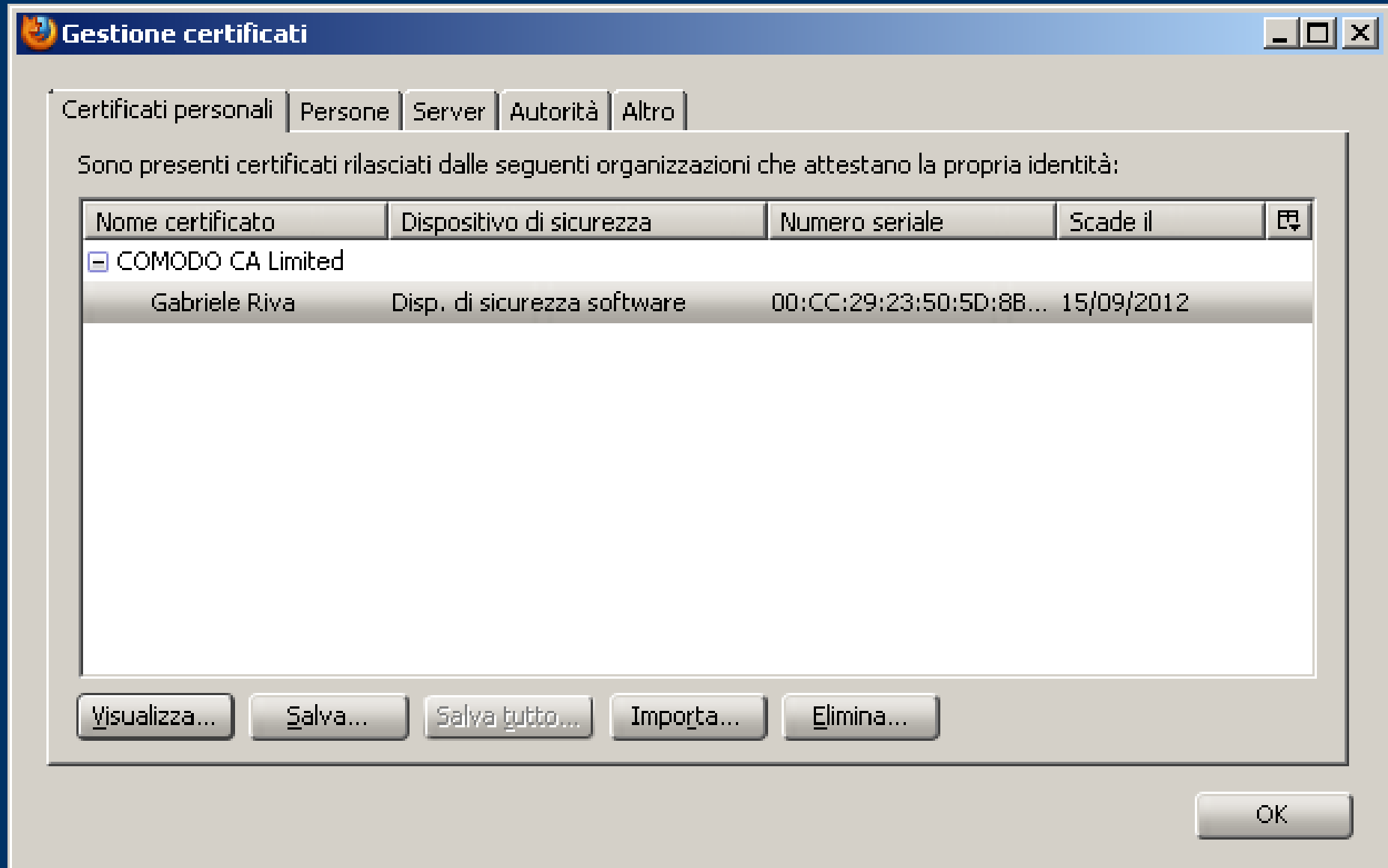
- Internet Explorer: Strumenti > Opzioni Internet > Contenuto “Certificati”
- Selezionare il certificato e cliccare su esporta

Come esportare il certificato in Internet Explorer



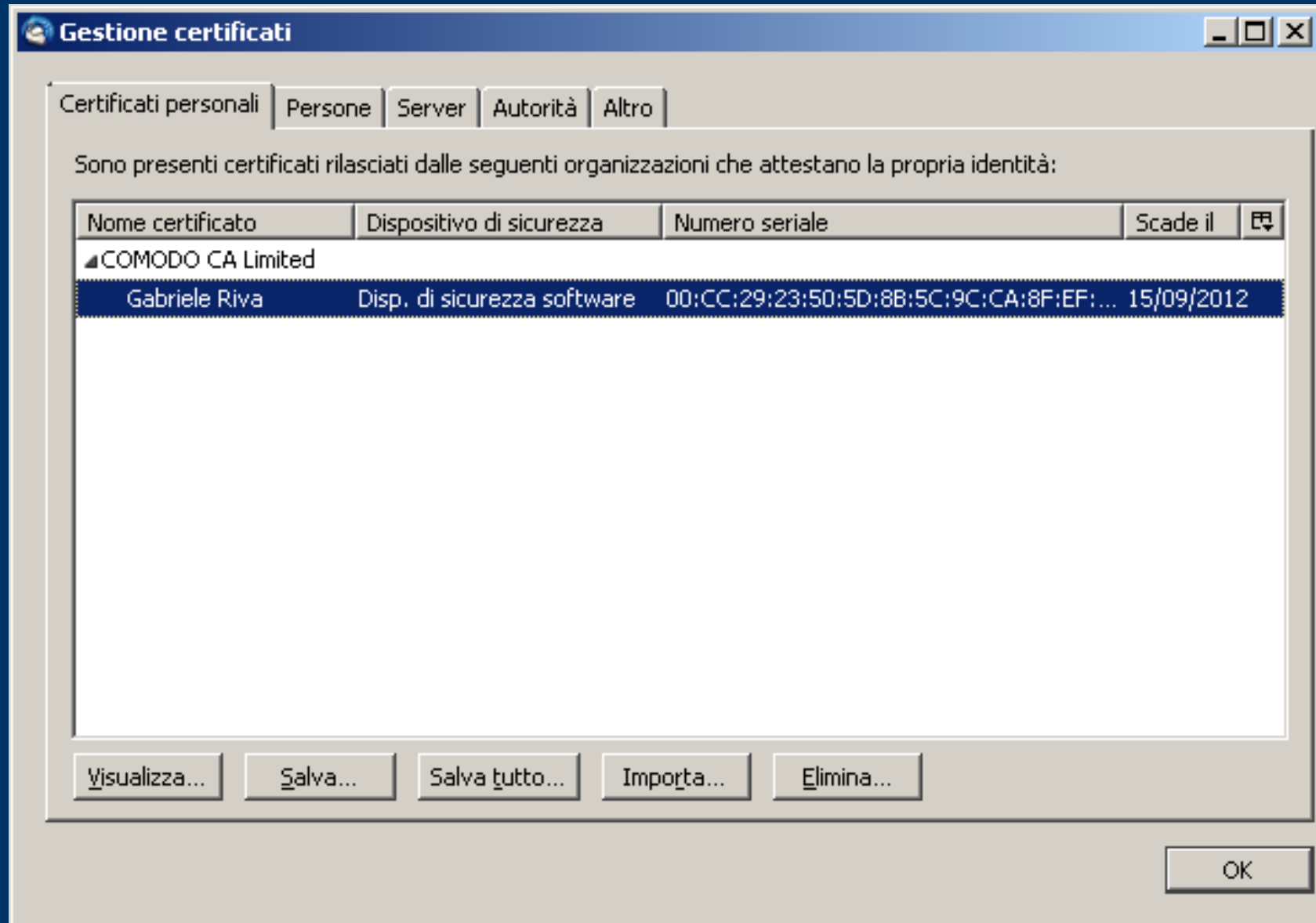
Come esportare il certificato in Firefox

Opzioni > Avanzate > Mostra certificati, selezionare il certificato e cliccare su Salva



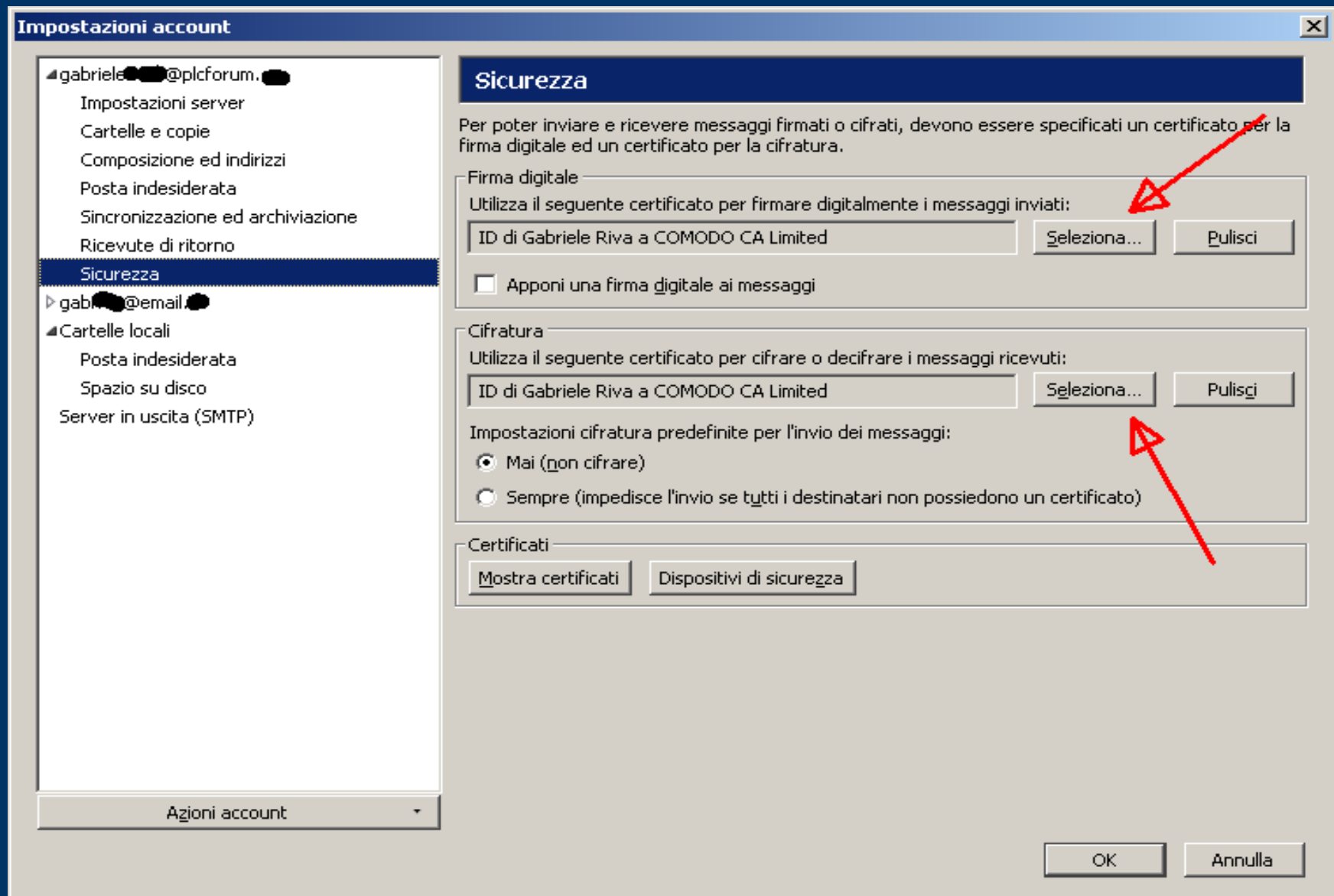
Come importare il certificato in Thunderbird

Strumenti > Opzioni > Avanzate > Mostra certificati, cliccare su Importa



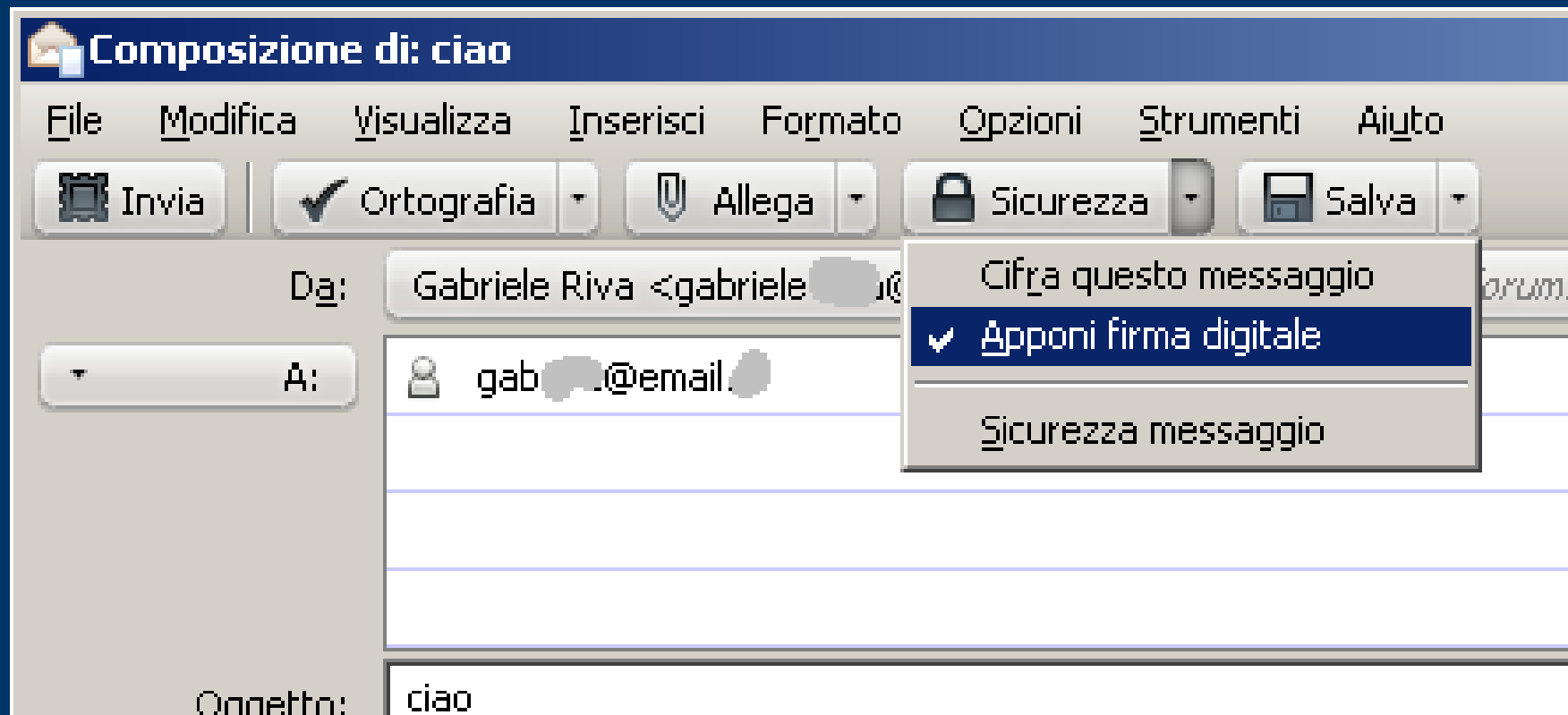
Impostare il certificato per la firma in e-mail

Strumenti > Impostazioni account > Sicurezza (selezionare il certificato)



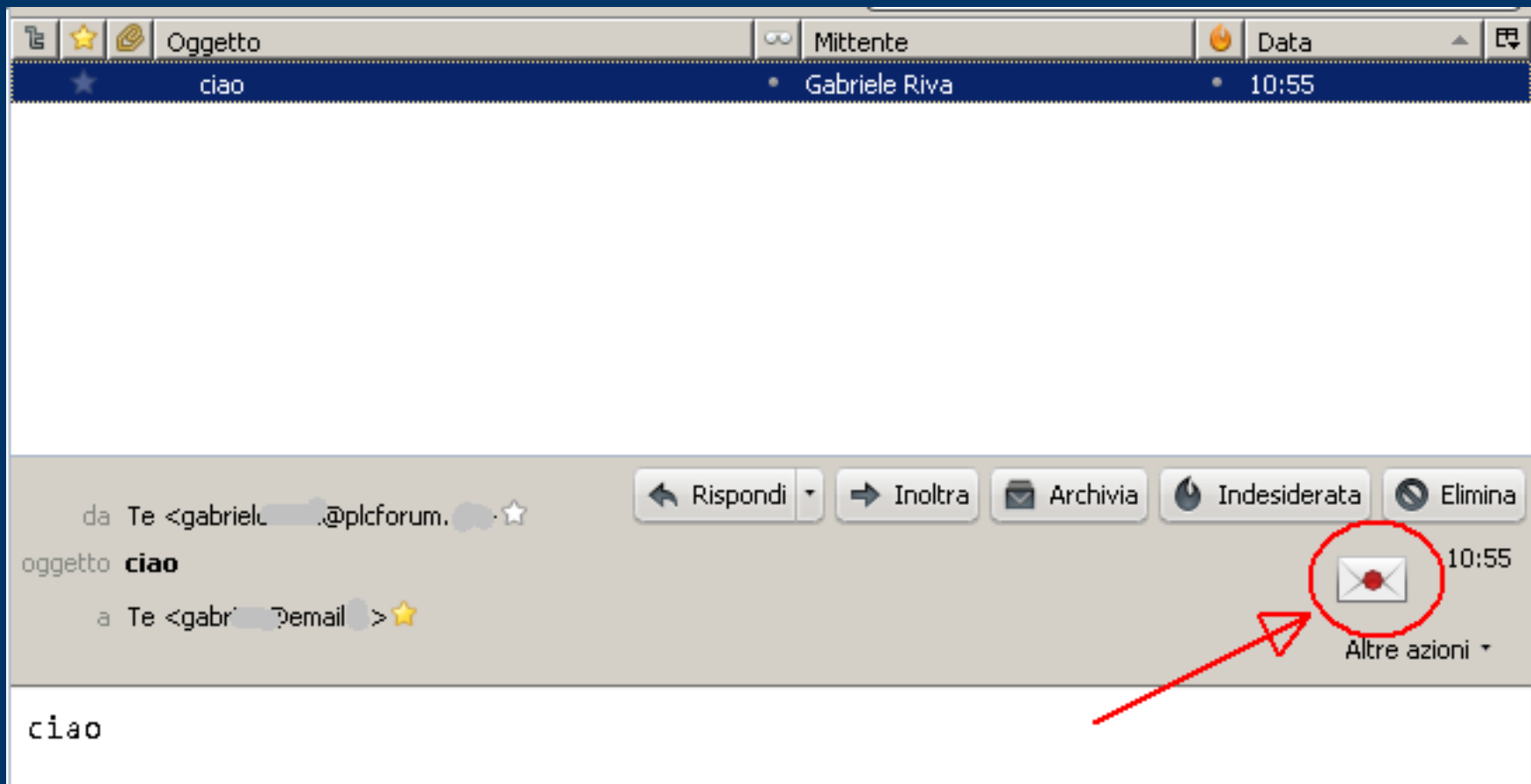
Inviare e-mail con firma digitale

Scrivi > Sicurezza selezionare “Apponi firma digitale”



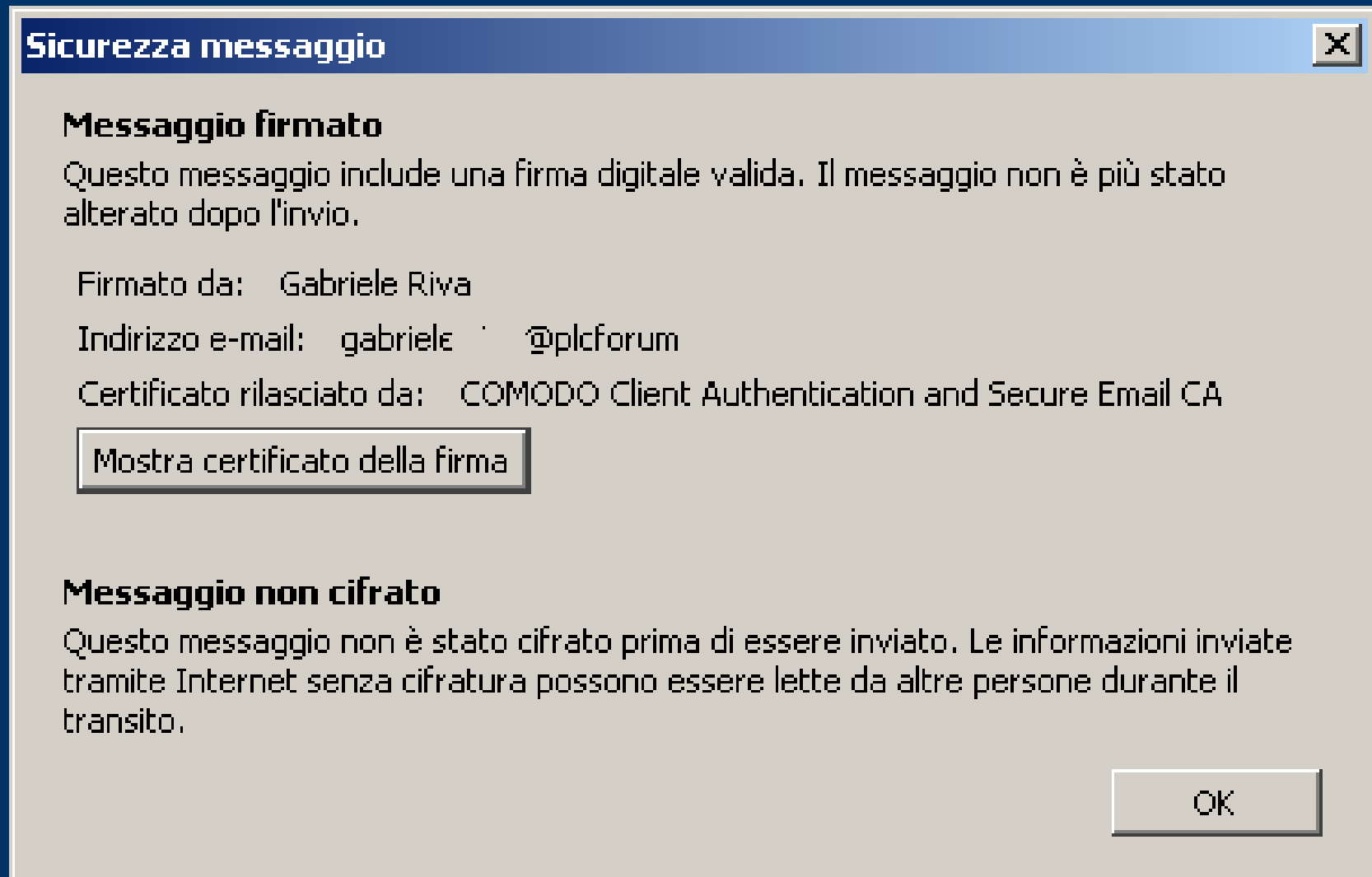
Inviare e-mail con firma digitale

Ecco come appare l'email ricevuta, notare la busta con il sigillo.



Inviare e-mail con firma digitale

Cliccando sulla busta vengono mostrate le informazioni di firma con la possibilità di visualizzare il certificato del mittente.



▣ *Posta elettronica certificata*

La Posta Elettronica Certificata (PEC) è il sistema che consente di inviare e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno, come stabilito dalla vigente normativa (DPR 11 Febbraio 2005 n.68).

Benché il servizio PEC presenti forti similitudini con la tradizionale Posta Elettronica, è doveroso dare risalto alle caratteristiche aggiuntive, tali da fornire agli utenti la certezza – a valore legale - dell'invio e della consegna (o della mancata consegna) delle e-mail al destinatario.

La Posta Elettronica Certificata ha il medesimo valore legale della raccomandata con ricevuta di ritorno con attestazione dell'orario esatto di spedizione.

Inoltre, il sistema di Posta Certificata, grazie ai protocolli di sicurezza utilizzati, è in grado di garantire la certezza del contenuto non rendendo possibili modifiche al messaggio, sia per quanto riguarda i contenuti che eventuali allegati.

La Posta Elettronica Certificata garantisce - in caso di contenzioso - l'opponibilità a terzi del messaggio.

☐ *Posta elettronica certificata*

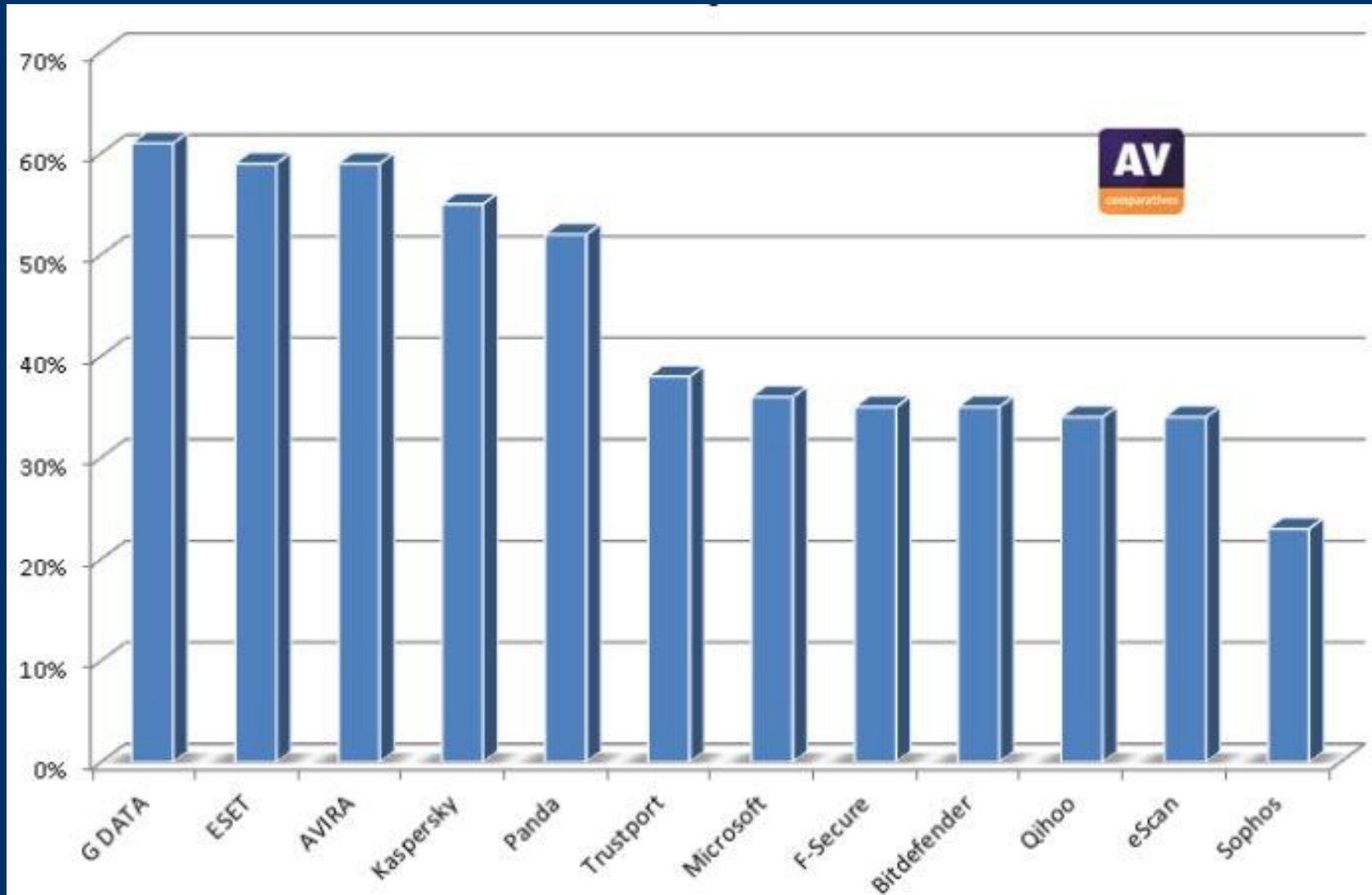
Il termine "Certificata" si riferisce al fatto che il gestore del servizio rilascia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio ed eventuali allegati. Allo stesso modo, il gestore della casella PEC del destinatario invia al mittente la ricevuta di avvenuta consegna. I gestori certificano quindi con le proprie "ricevute" che il messaggio:

- E' stato spedito
- E' stato consegnato
- Non è stato alterato

In ogni avviso inviato dai gestori è apposto anche un riferimento temporale che certifica data ed ora di ognuna delle operazioni descritte. I gestori inviano ovviamente avvisi anche in caso di errore in una qualsiasi delle fasi del processo (accettazione, invio, consegna) in modo che non possano esserci dubbi sullo stato della spedizione di un messaggio. Nel caso in cui il mittente dovesse smarrire le ricevute, la traccia informatica delle operazioni svolte, conservata dal gestore per 30 mesi, consentirà la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.

Antivirus

Un antivirus è un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi (malware) come worm, trojan e dialer.



☐ *Antivirus*

Avast! - **Avira AntiVir** – aVtomic - BullGuard
Antivirus – **ClamAV** - Comodo Antivirus - Computer
Associates (CA) - Emsisoft Anti-Malware - NOD32 -
Frisk Software – F-Secure - G Data Software AG –
GeCAD - **AVG Anti-Virus** – Hauri – H+BEDV –
Kaspersky – McAfee - **Microsoft Security
Essentials** – Mks – Norman - Panda (antivirus) - PC
Tools - Quick Heal - Aladdin Knowledge Systems –
BitDefender - aVtomic AntiVirus – Sophos - Norton
Antivirus - VirIT eXplorer - Trend Micro - Vipre -
VBA32 ANTI-VIRUS - ZoneAlarm AntiVirus