

"InfoCamere"
Società Consortile di Informatica delle Camere di Commercio Italiane per azioni

LEGALMAIL Posta Certificata
Manuale utente



Indice

1.Termini e definizioni	3
2.LEGALMAIL – Posta Certificata	4
2.1Caratteristiche dei messaggi.....	4
2.1.1Messaggio di posta certificata.....	4
2.1.2Messaggio da posta normale a posta certificata.....	7
2.1.3Messaggio da posta certificata a posta normale.....	8
2.2Note e particolarità dei messaggi di posta certificata.....	9
3.Accesso a LEGALMAIL	10
3.1Accesso al sistema WEBMAIL attraverso il sito LEGALMAIL.....	10
3.2Accesso a Webmail.....	12
3.3La maschera Principale: La mia posta.....	13
3.3.1Ricezione di messaggi crittografati.....	19
3.4Nuovo Messaggio.....	20
3.4.1Modalità Normale.....	20
3.4.2Modalità avanzata.....	22
3.5Rubrica.....	24
3.6Opzioni.....	27
3.7Guida.....	30
4.Esempi di messaggi di posta certificata	31
4.1Ricevuta di Accettazione.....	31
4.2Messaggio di Posta Certificata.....	34
4.3Ricevuta di Consegna.....	36
4.4Anomalia di messaggio.....	37
5.Requisiti Tecnici e Configurazione Client / Browser	38
5.1Requisiti tecnici.....	38
5.2Accesso via Webmail.....	40
5.3Accesso via client.....	40
5.3.1Configurazione Outlook Express con Internet Explorer 5.5 o superiore.....	42

1. Termini e definizioni

AOO	Area Organizzativa Omogenea
Browser	Software su stazione di lavoro per la navigazione in WEB
WEB	Architettura Intranet, Extranet, Internet
Punto di accesso	Componente del servizio di posta elettronica certificata che fornisce i servizi di accesso per l'invio di messaggi di posta certificata, i servizi di accesso dell'utente, l'emissione della ricevuta di accettazione. Realizza inoltre l'imbustamento del messaggio originale nel messaggio di trasporto.
Punto di ricezione	Componente del servizio di posta elettronica certificata che riceve il messaggio all'interno di un dominio di posta certificata: corrisponde al sistema di posta elettronica destinato alla ricezione dei messaggi per il dominio di posta certificata, effettua i controlli sulla provenienza/correttezza del messaggio, emette la ricevuta di presa in carico ed imbusta i messaggi errati in un messaggio di anomalia di trasporto.
Punto di consegna	Componente del servizio di posta certificata che effettua la consegna del messaggio nella casella di posta elettronica certificata. Inoltre, effettua i controlli sulla provenienza/correttezza del messaggio ed emette la ricevuta di avvenuta consegna.
Ricevuta di accettazione	Ricevuta rilasciata al mittente dal gestore di posta certificata di riferimento del mittente. La ricevuta è sempre sottoscritta con firma elettronica dal gestore di posta certificata mittente e contiene i dati di certificazione che attestano l'invio del messaggio.
Ricevuta di avvenuta consegna	Ricevuta rilasciata al mittente dal gestore di posta certificata di riferimento del destinatario; la ricevuta è sempre sottoscritta con firma elettronica dal gestore di posta certificata destinatario e contiene i dati di certificazione che attestano l'avvenuta consegna nella casella di posta certificata destinataria e (per i destinatari in "to") la copia completa del messaggio.
Ricevuta di presa in carico	Quando la trasmissione del documento avviene tra due diversi gestori, il gestore del destinatario rilascia al gestore del mittente la ricevuta che attesta l'avvenuta presa in carico del messaggio. L'informazione coinvolge i due gestori mentre l'utente non riceverà alcuna comunicazione.

2. LEGALMAIL – Posta Certificata

L'utilizzo di caselle di posta elettronica certificata Legalmail garantisce l'accesso sicuro alla propria casella di posta elettronica sia attraverso un client di posta sia direttamente da Internet attraverso i più comuni browser.

L'applicazione sviluppata da InfoCamere per accedere alla posta certificata via browser è detta WebMail.

Legalmail, sistema di Posta Certificata, consente di:

- accedere in sicurezza alla casella di posta da client di posta o da browser
- spedire / ricevere messaggi con client di posta o con browser
- firmare e crittografare i messaggi (utilizzando smartcard InfoCamere) attraverso Webmail (in ambiente windows) o il client di posta
- ricevere messaggi (ricevute) che diano garanzie all'utente sull'invio e sull'avvenuta consegna del messaggio al destinatario

Legalmail è stata realizzata in conformità alle norme sancite nel D.P.R. del 28 dicembre 2000, n. 445 art. 14 comma 1, 2, e 3 ed alle specifiche dettate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).

2.1 Caratteristiche dei messaggi

La posta certificata permette di scambiare messaggi tra utenti con caselle di posta certificata e utenti con caselle di posta non certificata: è necessario però ricordare che un messaggio si intende di posta certificata solo se mittente e destinatario hanno entrambi una casella di posta certificata. In caso contrario non si ottengono tutte le garanzie previste e l'utente non riceverà tutte le ricevute tipiche della posta certificata. Inoltre per ciascun messaggio inviato da una casella di posta certificata è necessario almeno un destinatario in "TO".

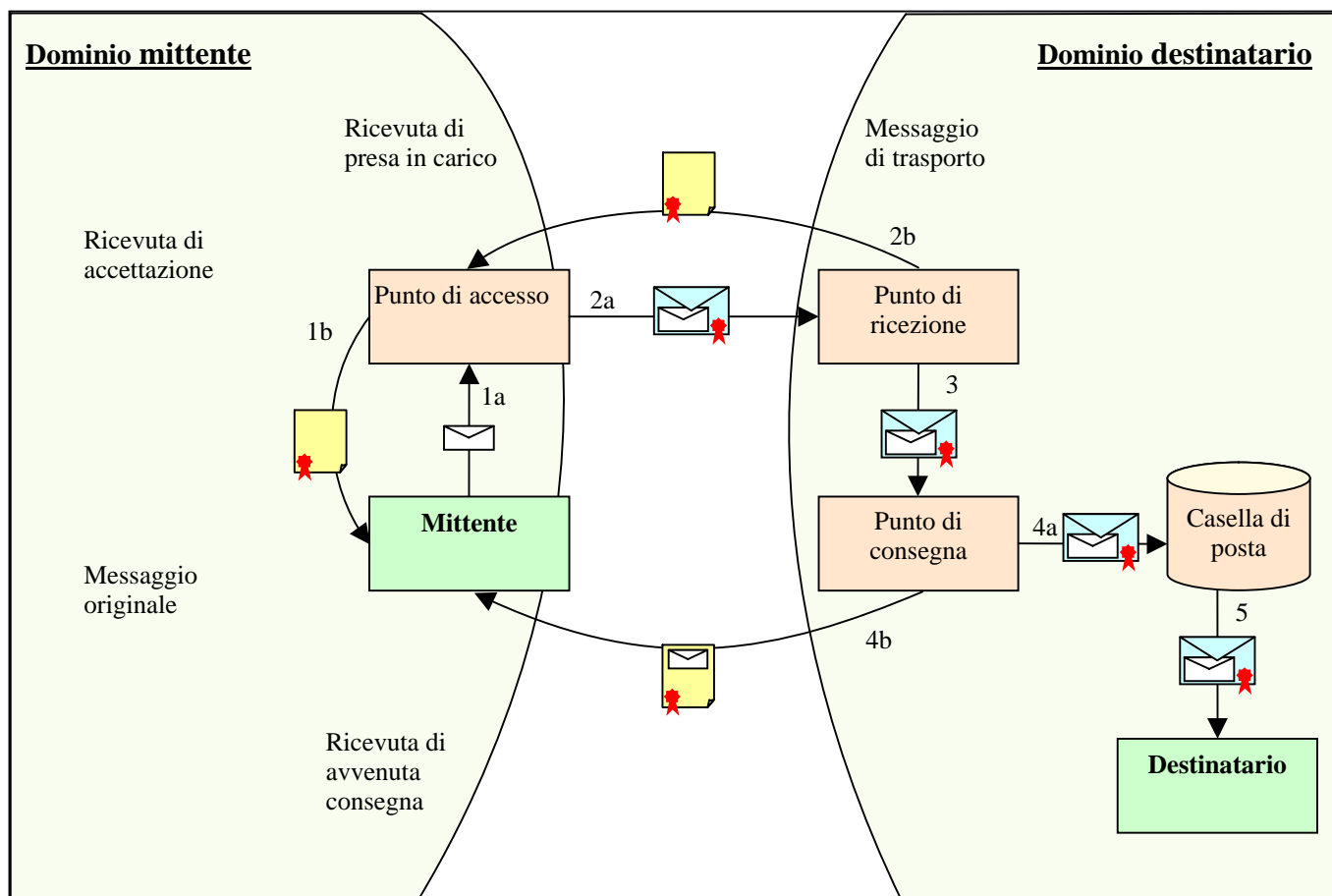
2.1.1 Messaggio di posta certificata

Il messaggio di posta certificata, nel "tragitto" dal mittente al destinatario, viene elaborato dai gestori della posta elettronica certificata (provider) in modo diverso rispetto ai normali messaggi di posta elettronica. Le attività si possono riassumere in 5 punti (cfr. grafico):

- 1) Il mittente invia il suo messaggio e riceve la **ricevuta di accettazione**;
- 2) Il messaggio passa dal provider del mittente a quello del destinatario;
- 3) Il messaggio passa dal sistema di ricezione del provider destinatario al sistema che gestisce le caselle di posta del provider destinatario (i due sistemi potrebbero essere molto lontani; per esempio nel caso di Pubblica Amministrazione con sede centrale e molte sedi sul territorio);
- 4) Il messaggio viene inserito nella casella del destinatario e viene inviata la **ricevuta di consegna** al mittente;

5) Il destinatario accede alla propria casella per leggere i messaggi ricevuti.

Lo schema sotto riportato descrive sinteticamente le operazioni svolte su un **messaggio di posta certificata** che transita da un provider ad un altro.



Qui di seguito sono descritti i flussi con alcuni dettagli aggiuntivi

La numerazione dei punti si riferisce allo schema sopra riportato.

1a – Il mittente invia il messaggio al suo provider (punto di accesso) che lo riceve;

1b – Il provider effettua dei controlli sul messaggio; se non riscontra problemi, invia al mittente una ricevuta di accettazione, firmata digitalmente, in cui indica quali sono i destinatari che appartengono alla posta certificata e quali sono quelli esterni; per questi ultimi la trasmissione non viene considerata di posta certificata. La ricevuta contiene la data e l'ora di elaborazione (data e ora di invio) e deve essere conservata dall'utente.

Non vengono accettati messaggi con destinatari in BCC / CCN (copia nascosta)

2a – Il provider del mittente (punto di accesso) crea un messaggio di trasporto a cui viene allegato il messaggio originale; il messaggio di trasporto contiene alcune informazioni sulla trasmissione, tra cui la data e l'ora di invio. Il messaggio di trasporto viene firmato dal provider mittente e spedito al destinatario.

2b - Il provider del destinatario (punto di ricezione) controlla il messaggio ricevuto, in particolare la firma del provider mittente.

- Se il messaggio è integro e il mittente è presente nell'indice dei gestori di posta certificata, viene inviata una ricevuta di presa in carico al provider del mittente. Il messaggio prosegue come messaggio di posta certificata.
- In caso contrario, il messaggio viene trattato come un messaggio di posta non certificata (si veda [Messaggio da posta normale a posta certificata](#)).

3 – Il messaggio di trasporto, con allegato il messaggio originale, viene inoltrato al sistema che gestisce le caselle di posta (punto di consegna). Il tutto avviene all'interno del provider destinatario: in molti casi i punti di ricezione e di consegna possono coincidere.

4a – Il provider del destinatario (punto di consegna) deposita nella casella del destinatario il messaggio di trasporto con allegato il messaggio originale.

4b- Se la consegna va a buon fine, il provider del destinatario invia al mittente una ricevuta di consegna, firmata digitalmente. Se il destinatario è primario (in "to" e non in "cc") la ricevuta contiene, in allegato, tutto il messaggio originario. La ricevuta di consegna rappresenta la prova principale in mano al mittente e va conservata accuratamente. Infatti contiene data e ora di consegna e contenuto consegnato: il tutto firmato dal provider di posta certificata che ha effettuato la consegna.

Se la consegna non va a buon fine (casella inesistente, piena, eccetera) viene inviata al mittente una comunicazione di errore.

Attenzione: prima di spedire un messaggio è bene verificare di avere **spazio** sufficiente per ricevere tutte le ricevute di consegna. Se il messaggio viene inviato (in "TO") a molti destinatari di posta certificata e la dimensione del messaggio è significativa si deve considerare che ogni ricevuta di consegna ha in allegato tutto il messaggio inviato. Per acquisire correttamente tutte le ricevute di consegna si deve avere quindi spazio sufficiente.

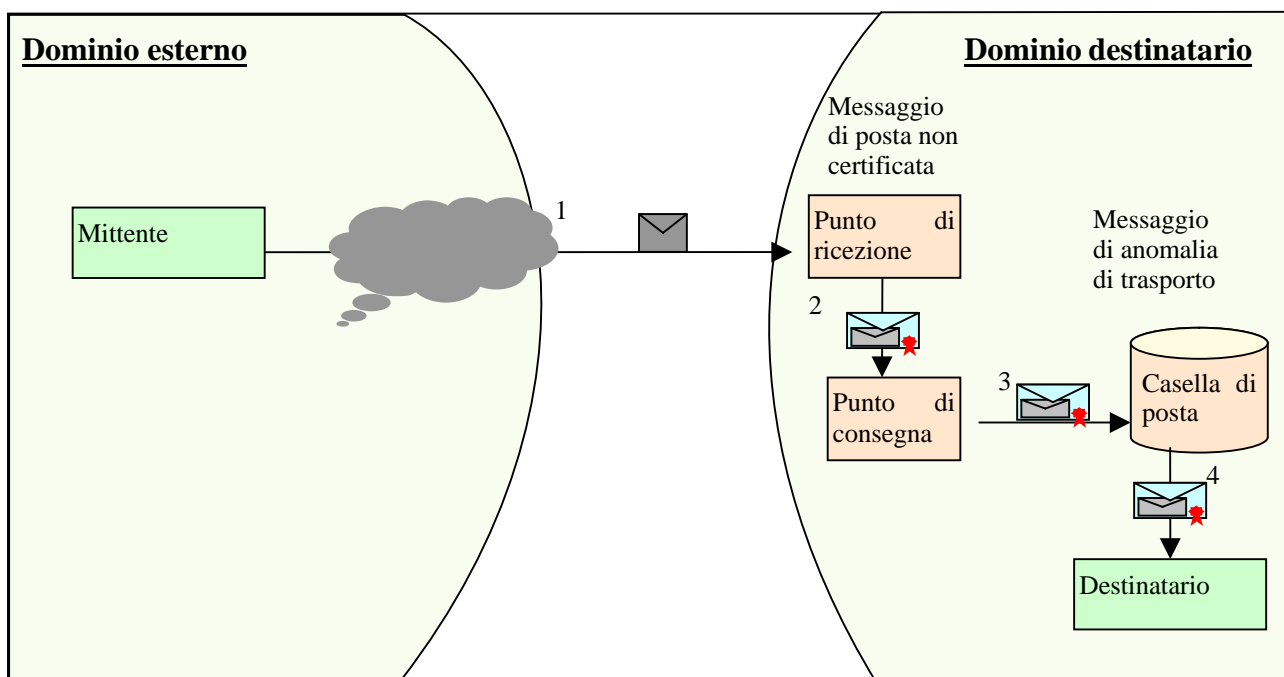
5 – Il destinatario accede alla propria casella di posta certificata e legge il messaggio. Il messaggio ricevuto è il messaggio di trasporto con allegato il messaggio originale.

I messaggi ricevuti da posta certificata, malgrado le apparenze, non sono spediti dal mittente originale, ma dal suo provider di posta certificata.

2.1.2 Messaggio da posta normale a posta certificata

In questo paragrafo viene descritto l'iter di un messaggio di posta normale inviato verso una casella di posta certificata (i numeri tra parentesi si riferiscono alla figura sotto riportata).

1. L'utente invia un messaggio di posta elettronica da una casella di posta non certificata. Il messaggio è indirizzato ad una casella di posta certificata e perviene ad un provider di posta certificata (punto di ricezione) (1)
2. Il punto di ricezione non riconosce le caratteristiche del messaggio di posta certificata e quindi crea un messaggio di anomalia, firmato digitalmente, a cui allega il messaggio ricevuto. Il messaggio di anomalia viene inoltrato al punto di consegna (se diverso dal punto di ricezione) (2)
3. Il messaggio di anomalia, a cui è allegato il messaggio ricevuto, viene depositato nella casella del destinatario (3).
4. Il destinatario accede alla casella di posta e legge il messaggio di anomalia che contiene il messaggio originale (4).



Nota:

I messaggi di posta certificata che non vengono riconosciuti come tali dal provider del destinatario (punto di ricezione) vengono trattati come messaggi di posta non certificata.

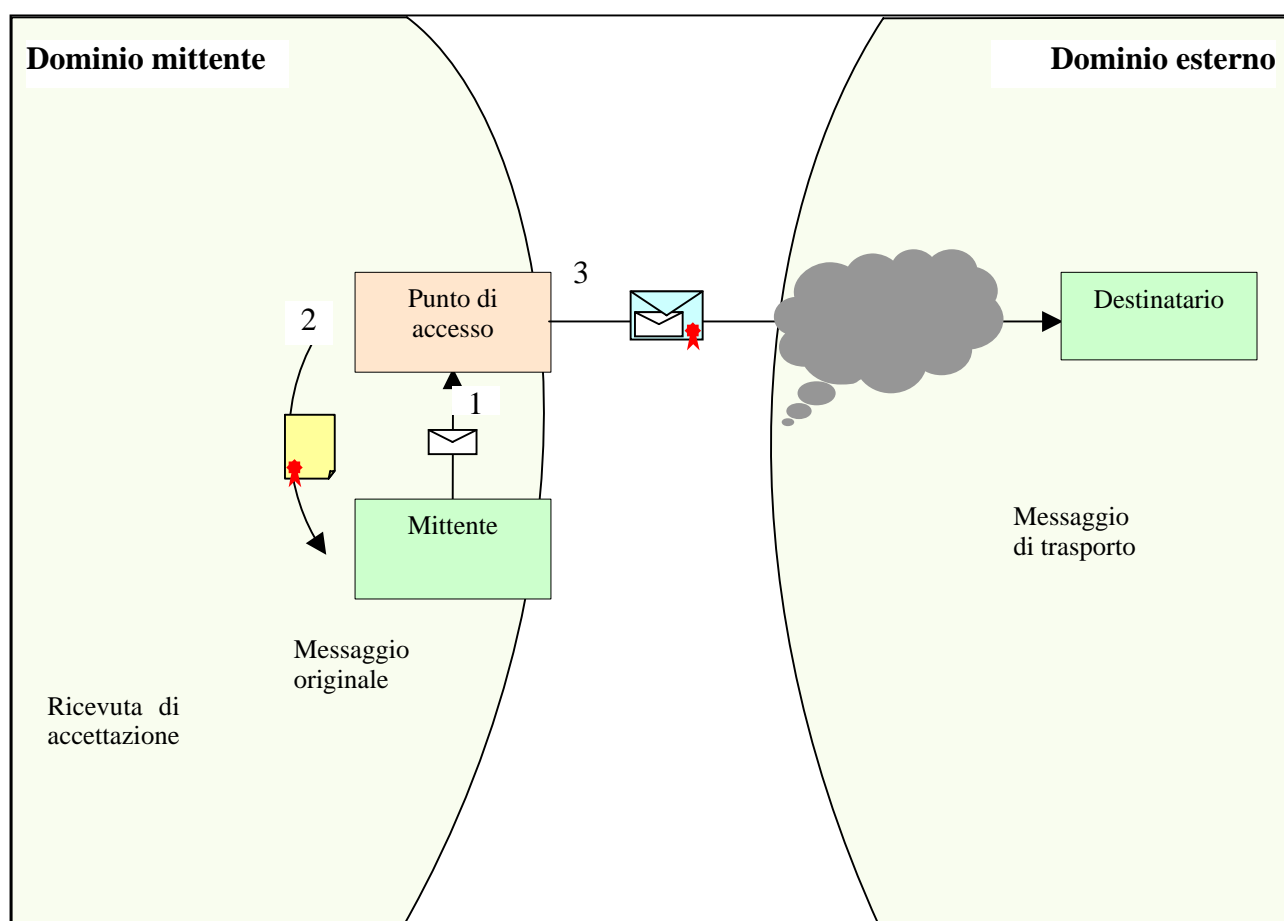
2.1.3 Messaggio da posta certificata a posta normale

In questo paragrafo viene descritto l'iter di un messaggio di posta certificata inviato verso una casella di posta normale (i numeri tra parentesi si riferiscono alla figura sotto riportata).

1. Il mittente invia il messaggio al suo provider (punto di accesso) che lo riceve (1).
2. Il provider effettua dei controlli sul messaggio; se non rileva problemi, invia al mittente una ricevuta di accettazione, firmata digitalmente, in cui indica quali sono i destinatari che appartengono alla posta certificata e quali sono quelli esterni (per questi ultimi la trasmissione non viene considerata di posta certificata). La ricevuta contiene la data e l'ora di elaborazione (data e ora di invio) (2).

Non vengono accettati messaggi con destinatari in BCC (copia nascosta)

3. Il provider del mittente (punto di accesso) crea un messaggio di trasporto a cui viene allegato il messaggio originale; il messaggio di trasporto contiene alcune informazioni sulla trasmissione, tra cui la data e l'ora di invio. Il messaggio di trasporto viene firmato dal provider mittente e spedito al destinatario (3).



Note:

Il provider destinatario, non essendo un provider di posta certificata, consegna il messaggio di trasporto senza effettuare controlli, senza fornire ricevute di consegna e senza tenere log particolari.

Il destinatario accede alla propria casella di posta e legge il messaggio. Il messaggio ricevuto è il messaggio di trasporto con allegato il messaggio originale.

2.2 Note e particolarità dei messaggi di posta certificata

Il servizio prevede alcune ricevute che diano garanzie all'utente sull'invio e sull'avvenuta consegna del messaggio al destinatario. Queste ricevute sono prodotte da Legalmail secondo le specifiche contenute nelle regole per la posta certificata pubblicate in internet sul sito del Centro Tecnico del CNIPA.

Si ricorda che: 1) un messaggio si intende di posta certificata solo se mittente e destinatario hanno entrambi una casella di posta certificata; 2) in base alle regole di posta certificata, non sono ammessi messaggi che non contengano almeno un destinatario in "TO".

Inoltre non è prevista la firma del destinatario per l'accettazione del messaggio in forza di quanto previsto dall'articolo 14 comma 1 del dpr 445 del 2000 (Il documento informatico ... "si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato").

La posta certificata fornisce garanzie sulla trasmissione del messaggio ma non certifica l'identità del mittente. Per avere la certezza dell'identità del mittente si devono utilizzare, insieme alla posta certificata, anche strumenti di firma digitale. La posta certificata Legalmail permette l'utilizzo di firma e crittografia dei messaggi sia da client sia da Webmail. Inoltre è possibile inviare messaggi allegando documenti firmati con la firma di sottoscrizione a norme CNIPA.

Per le caratteristiche proprie della posta certificata, ogni messaggio inviato da Legalmail posta certificata è firmato digitalmente dal gestore di posta certificato del mittente. L'utente può, a sua discrezione, inviare i messaggi secondo diverse modalità a seconda del valore e del contenuto del messaggio. L'utente può quindi scegliere di:

- inviare un semplice messaggio (che sarà firmato digitalmente dal provider); questo invio dà garanzie sulla trasmissione.
- inviare un messaggio firmandolo digitalmente attraverso la propria smartcard rilasciata da InfoCamere (il messaggio risulterà firmato dal gestore mittente e dal mittente; in questo modo si avranno garanzie sulla trasmissione e sull'identità del mittente)
- inviare un messaggio crittografato (il messaggio sarà firmato digitalmente dal provider dando quindi garanzie sulla trasmissione e sarà crittografato dall'utente per una maggiore riservatezza dell'informazione).
- inviare un messaggio firmato digitalmente e crittografato (questo messaggio riassume le caratteristiche di tutti i punti precedenti)

Inoltre l'utente può decidere di allegare documenti firmati digitalmente: la firma dà garanzie sul documento allegato.

Le attestazioni temporali date dalla posta certificata sono allineate, a meno di un secondo, con un riferimento di tempo ufficiale.

Nel cap.4, [Esempi di messaggi di posta certificata](#), sono riportati esempi di messaggi con la descrizione delle ricevute prodotte.

Attenzione: i messaggi ricevuti da posta certificata, malgrado le apparenze, non sono spediti dal mittente originale ma dal suo provider di posta certificata. In certe operazioni particolari si deve tener conto di questa caratteristica. Per esempio: se si intende aggiungere il mittente alla propria rubrica, l'operazione va effettuata nel messaggio allegato (postacert.eml). Altrimenti, malgrado l'intestazione del nome in rubrica sembri corretta, l'indirizzo inserito in rubrica non lo sarà: verrà inserito l'indirizzo del provider del mittente e i messaggi spediti non arriveranno mai alla giusta destinazione.

3. Accesso a LEGALMAIL

Per accedere alla casella di posta elettronica Legalmail, l'utente può utilizzare Webmail via browser oppure può utilizzare il proprio client di posta (opportunamente configurato).

Nei prossimi paragrafi sono descritte le caratteristiche di Webmail; l'accesso e l'utilizzo della casella di posta certificata attraverso client è specifico del client utilizzato dall'utente.

Si consiglia comunque di accedere a Webmail appena ricevuta la casella di posta per cambiare la password iniziale.

3.1 Accesso al sistema WEBMAIL attraverso il sito LEGALMAIL

Per accedere a Webmail è possibile collegarsi al sito www.legalmail.it: come si vede dalla maschera seguente è possibile accedere tramite user e password (LOGIN) o tramite smartcard con apposito certificato di autenticazione (LOGIN con CARD).

Legalmail "InfoCamere" La Posta Elettronica Certificata Home | Attivazione | Call-Center | FAQ

Cosa è Legalmail

Accesso alla casella

- Login
- Login con Card
- Configurazione

Il Servizio

- Caratteristiche
- Sicurezza
- Normativa

Ottenere una casella di Posta Elettronica Certificata oggi è semplice, immediato e vantaggioso

l'offerta

L'uso sempre più frequente della **posta elettronica**, in sostituzione dei tradizionali mezzi di trasmissione dei documenti (posta, fax, corriere), pone la necessità di disporre di un sistema **affidabile, sicuro e coerente con le norme** previste sulla documentazione amministrativa.

Il sistema Legalmail è la soluzione **InfoCamere** di Posta Elettronica Certificata (P.E.C.) realizzata per:

- garantire l'**identificazione certa del mittente**
- garantire l'**integrità e la confidenzialità del messaggio**
- certificare l'**avvenuto recapito** dello stesso: in questo modo i **messaggi di posta elettronica certificata equivalgono alla notificazione per mezzo della posta** nei casi consentiti dalla legge.

Legalmail è un servizio realizzato in conformità alle specifiche dettate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA)

Tutti i prodotti e servizi qui indicati sono forniti da [InfoCamere](#)

Se l'utente accede attraverso LOGIN, il sistema presenta la maschera di autenticazione a Webmail (cfr. [Accesso a Webmail](#))

Se invece l'utente accede attraverso LOGIN con CARD, il sistema avvisa l'utente riguardo il certificato di autenticazione che sta utilizzando e chiede di digitare il pin come dalla maschera seguente:



The screenshot shows a web browser window with the URL <http://1.71.4.114:8180/legalmail/index.jsp>. The page header features the "Legalmail" logo with the tagline "La Posta Elettronica Certificata" and the "InfoCamere" brand name. Navigation links for "Home", "Attivazione", "Call-Center", and "FAQ" are present.

The main content area is titled "Cosa è Legalmail" and features a large graphic with the text "Ottenerne una casella di Posta Elettronica Certificata". The graphic includes a blue folder icon with a white keyhole and a SmartCard. Below the graphic, the text explains that the use of electronic mail is the most frequent use of certified electronic mail, replacing traditional means of document transmission (post, fax, courier) and requiring a reliable, secure, and compliant system with administrative documentation norms.

The system Legalmail is the solution InfoCamere of Certified Electronic Mail (P.E.C.) realized for:

- garantire l'identificazione certa del mittente
- garantire l'integrità e la confidenzialità del messaggio
- certificare l'avvenuto recapito dello stesso: in questo modo i messaggi di posta elettronica certificata equivalgono alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Legalmail è un servizio realizzato in conformità alle specifiche dettate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA)

Tutti i prodotti e servizi qui indicati sono forniti da InfoCamere.

On the right side, there are two vertical navigation menus. The first, "Accesso alla casella", includes links for "Login", "Login con Card", and "Configurazione". The second, "Il Servizio", includes links for "Caratteristiche", "Sicurezza", and "Normativa".

3.2 Accesso a Webmail

Inserendo nell'apposita casella l'indirizzo www.webmail.infocamere.it, si accede alla videata di Login in cui l'utente deve farsi riconoscere dal sistema attraverso la propria Userid e Password:

Si giunge a questa stessa finestra anche selezionando LOGIN dal sito www.legalmail.it.



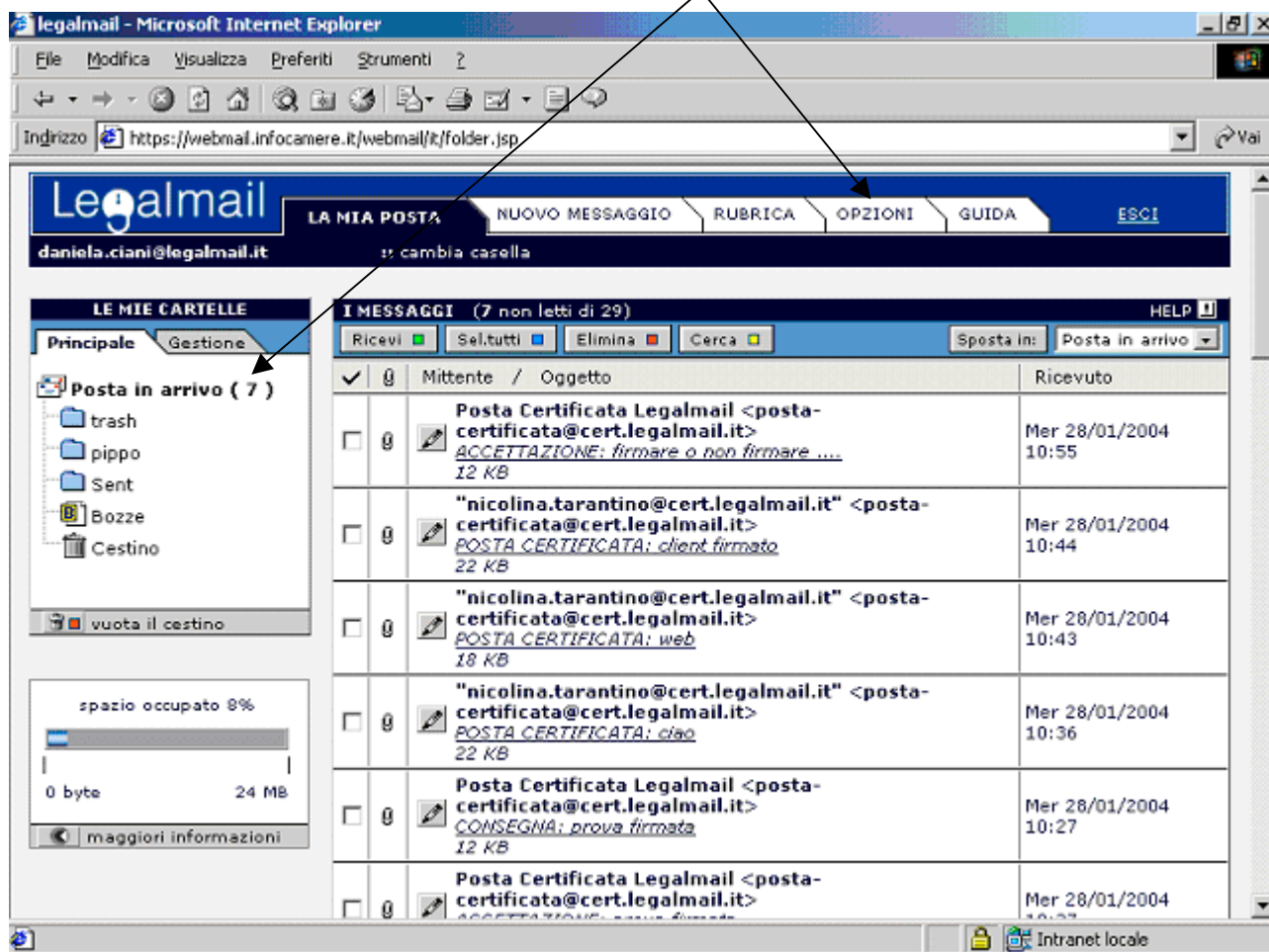
Se l'utente accede per la prima volta a Legalmail, è consigliabile cambiare la password fornita da InfoCamere selezionando la voce Cambio Password all'interno della linguetta Opzioni (cfr. [Opzioni](#))

Dopo aver immesso la propria Userid e Password (digitata in minuscolo) e cliccato sul tasto Conferma; comparirà la finestra con l'elenco dei messaggi ricevuti:

Per gli utenti che hanno più di una casella di posta Legalmail con la stessa utenza apparirà una finestra che permette di selezionare il servizio da utilizzare.

3.3 La maschera Principale: La mia posta

La finestra principale che appare subito dopo l'apertura di Webmail, è costituita dall'elenco dei messaggi ricevuti; nella parte alta si trovano 5 linguette per le diverse funzioni, le informazioni riguardo a quale cartella si sta consultando (di solito Posta in arrivo cioè la posta in entrata), il numero di messaggi di posta e l'help.



Messaggi ricevuti

La finestra presenta l'elenco dei messaggi ricevuti; ciascuna riga riporta l'indirizzo e-mail del mittente, l'indirizzo e-mail del provider di posta certificata mittente (se il messaggio è di posta certificata) l'oggetto e la dimensione del messaggio. Nella posta certificata l'oggetto dei messaggi contiene delle diciture standard che permettono una rapida identificazione del tipo di messaggio ricevuto:

- **POSTA CERTIFICATA:** indica che il messaggio ricevuto è di posta certificata;
- **ACCETTAZIONE:** è la ricevuta del gestore di posta certificata del mittente, che attesta l'invio di un messaggio;
- **CONSEGNA:** questo messaggio è generato dal gestore di posta certificata del destinatario e attesta che il messaggio del mittente è stato recapitato nella casella di posta del destinatario; la

ricevuta di consegna contiene anche la copia del messaggio inviato (se il destinatario era in "to").

- **ANOMALIA MESSAGGIO:** indica che il messaggio ricevuto non è di posta certificata

Nel caso l'utente riceva un messaggio di posta certificata da un altro sistema (diverso da Legalmail) non è necessario "trustare" il certificato di firma del provider mittente (cioè far riconoscere al sistema la validità del certificato di firma). Il sistema considera automaticamente validi i certificati di firma dei gestori di posta certificata.





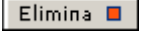

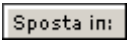

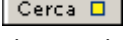

Il simbolo della penna accanto all'oggetto del messaggio indica che il messaggio è stato firmato digitalmente (dal gestore di posta certificata).

Nel caso il mittente abbia impostato (con Outlook) la richiesta di ricevuta di lettura, Webmail chiederà all'utente se accettare questa richiesta (in caso di risposta affermativa il sistema invia la ricevuta al mittente del messaggio appena aperto).

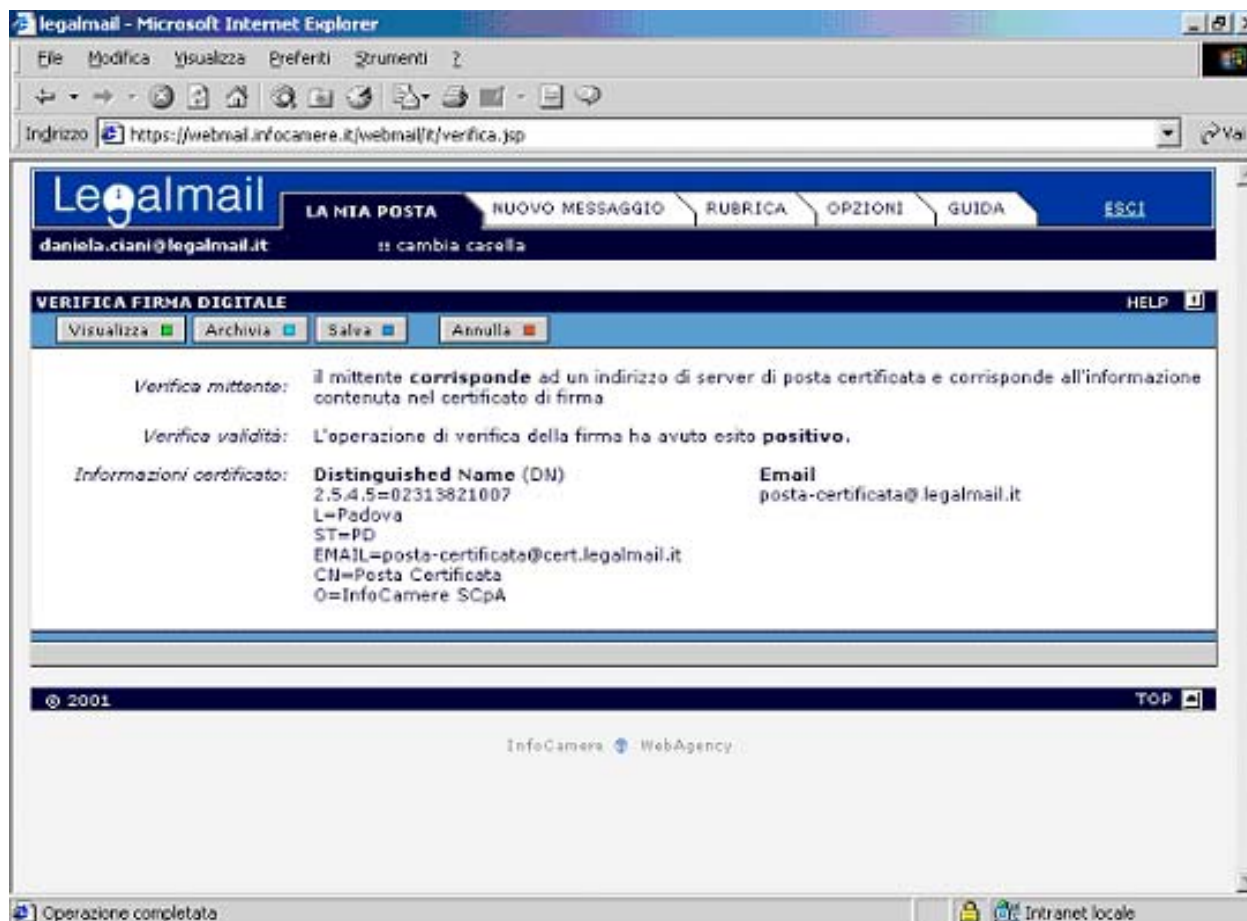
Inoltre per ragioni di sicurezza, se il messaggio contiene codice html con elementi "attivi" (per es. javascript, active-x, ...) il sistema non visualizza l'html, ma invita l'utente, se vuole vedere la pagina, a scaricare il messaggio sulla propria stazione di lavoro dove potrà visualizzarlo.

I messaggi possono essere ordinati secondo la selezione scelta nel menù a tendina nella barra in basso a sinistra "ordinati per": l'ordinamento può essere per data (dal più vecchio o dal più recente), per mittente o per destinatario (crescente o decrescente).





I bottoni in alto (come è possibile vedere nella maschera precedente) permettono di gestire i messaggi:

-  **Ricevi**  permette di ricevere i messaggi;
-  **Sel.tutti**  permette di selezionare o deselezionare tutti i messaggi della maschera;
-  **Elimina**  elimina dall'elenco i messaggi selezionati; i messaggi vengono spostati nella cartella trash (o in quella selezionata attraverso il menù opzioni, cfr. [Opzioni](#));
-  **Sposta in:**  permette di spostare i messaggi selezionati nella cartella scelta nel menù a destra del bottone;
-  **Cerca**  apre una "finestra" che consente la ricerca dei messaggi sulla base dei parametri di ricerca inseriti; i bottoni Cerca e Annulla consentono di effettuare la ricerca o tornare alla maschera precedente.

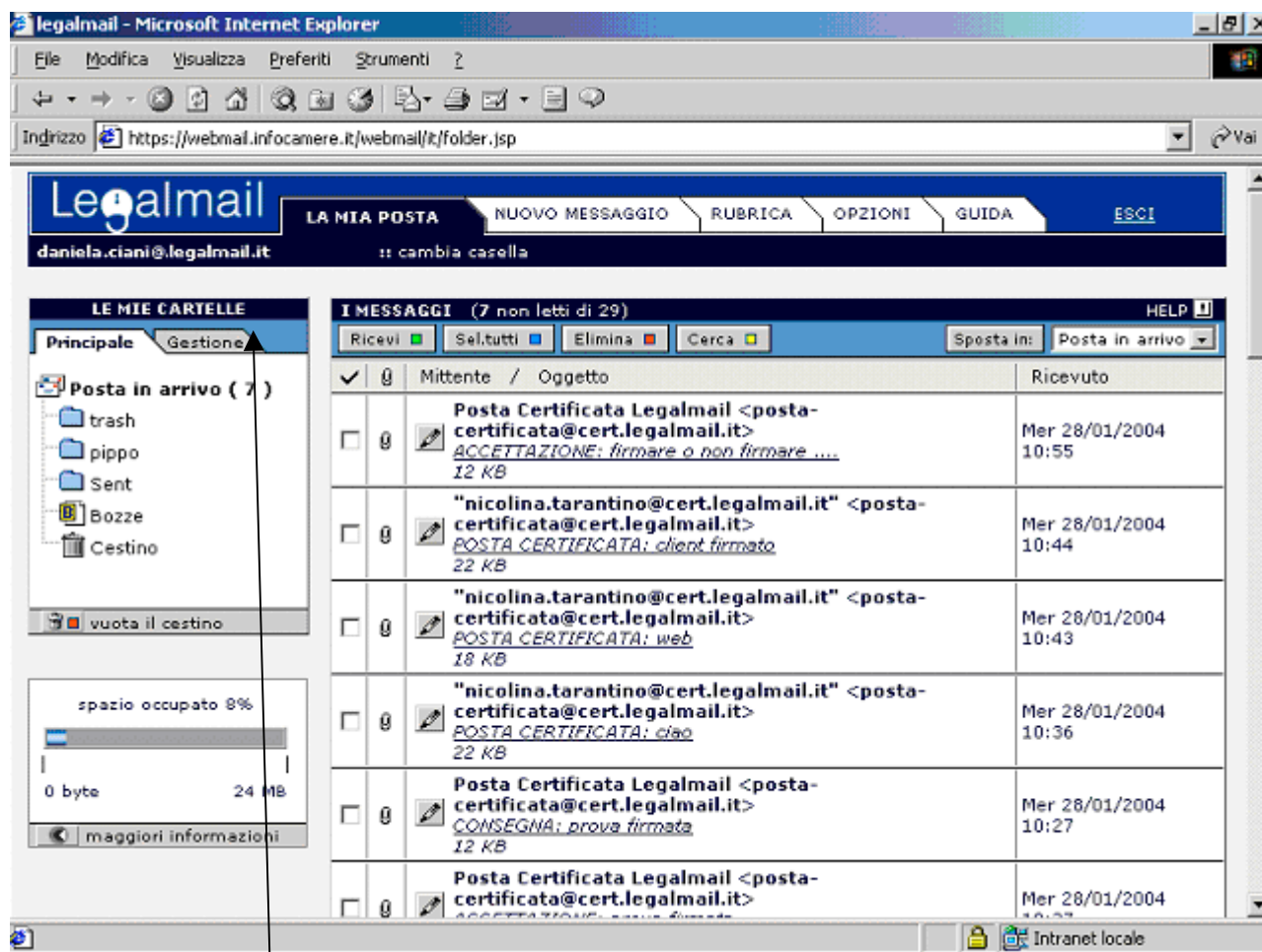
Cliccando sul bottone raffigurante una penna, che si trova a lato del messaggio è possibile verificare la firma digitale (del gestore di posta certificata) apposta sul messaggio corrispondente o importare i certificati (come è possibile vedere dalla maschera sotto riportata).



Nella parte alta della maschera si trovano i bottoni:

- **Visualizza**  appare una finestra con i dati completi relativi al certificato di firma
- **Archivia**  consente di salvare il certificato nella sezione Certificati (per inviare un messaggio crittografato è necessario aver ricevuto un messaggio firmato digitalmente dal destinatario)
- **Salva**  consente di salvare il certificato chiamato "cert.cer" sul disco locale
- **Annulla**  ritorna alla maschera precedente.

In modo analogo è possibile verificare la firma apposta dall'utente sul messaggio cliccando sul bottone "Sicurezza" (vedi maschera seguente). Durante la fase di verifica della firma il sistema controlla le liste di revoca di tutti i Certificatori.



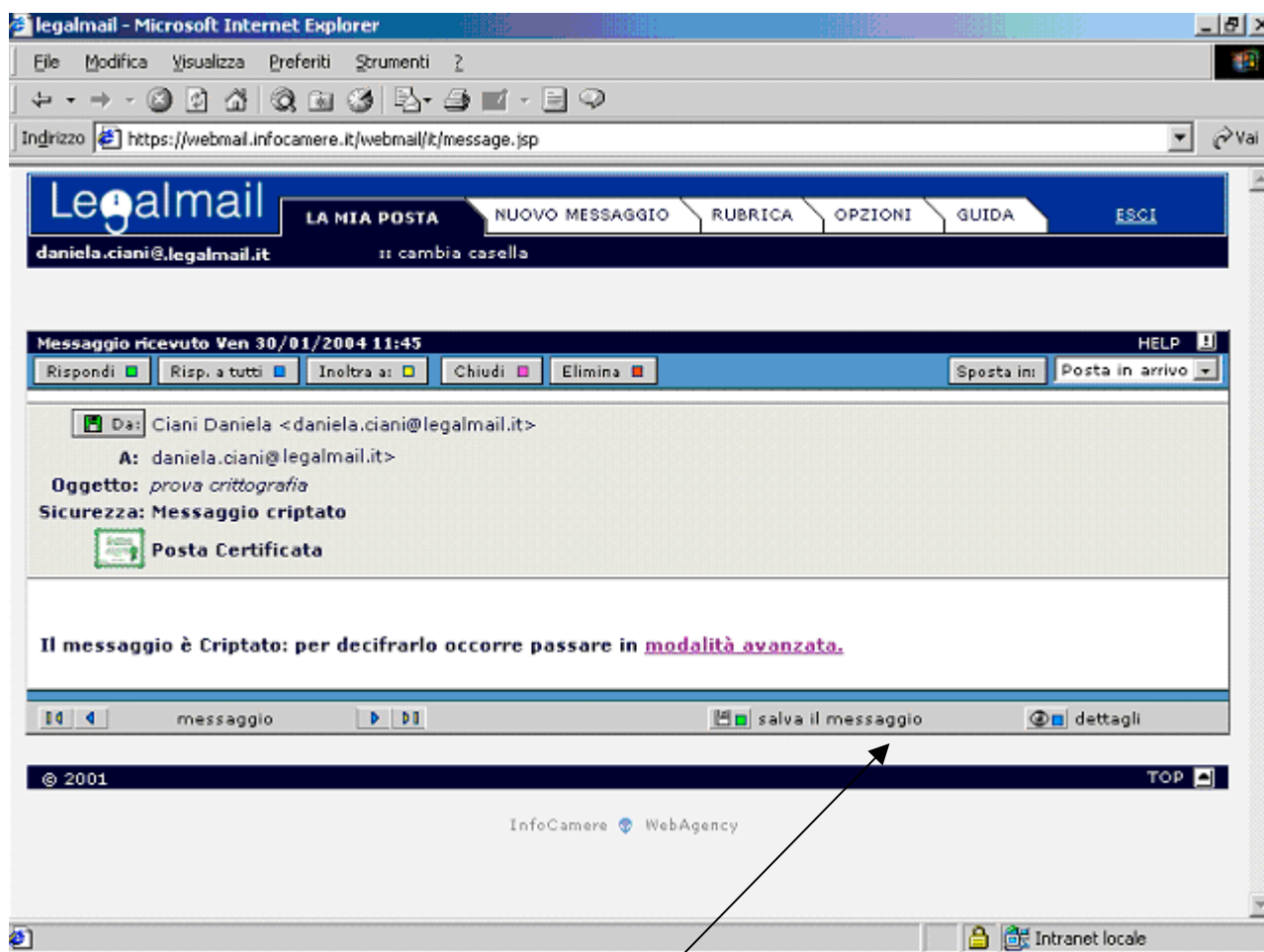
La sezione "Le mie Cartelle" serve per gestire le proprie cartelle della posta. Cliccando sul nome della cartella nella sezione **Principale**, si accede al contenuto della cartella stessa per poter consultare, cancellare ecc.. i messaggi.

Selezionando la sezione **Gestione** l'utente può creare, rinominare, spostare o eliminare le cartelle.

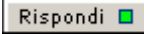
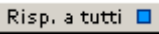
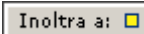
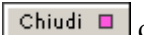
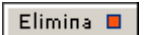


Per leggere un messaggio l'utente deve cliccare sull'oggetto del messaggio stesso.

Dopo aver cliccato sul messaggio da visualizzare comparirà una finestra per la visualizzazione e la gestione del messaggio: ogni messaggio, a seconda della sua tipologia, è costituito da alcune parti fisse descrittive, dagli allegati di posta certificata e dagli allegati al messaggio (alcuni esempi di messaggi di posta certificata sono consultabili al par. [Esempi di messaggi di posta certificata](#)).




Nel caso il messaggio sia stato crittografato è necessario utilizzare la modalità avanzata: se l'utente utilizza la modalità normale, un messaggio apposito lo avvisa di passare all'altra modalità (cfr. [Ricezione di messaggi crittografati](#))



Sulla finestra sono presenti alcuni bottoni per la gestione del messaggio (cfr. maschera seguente):

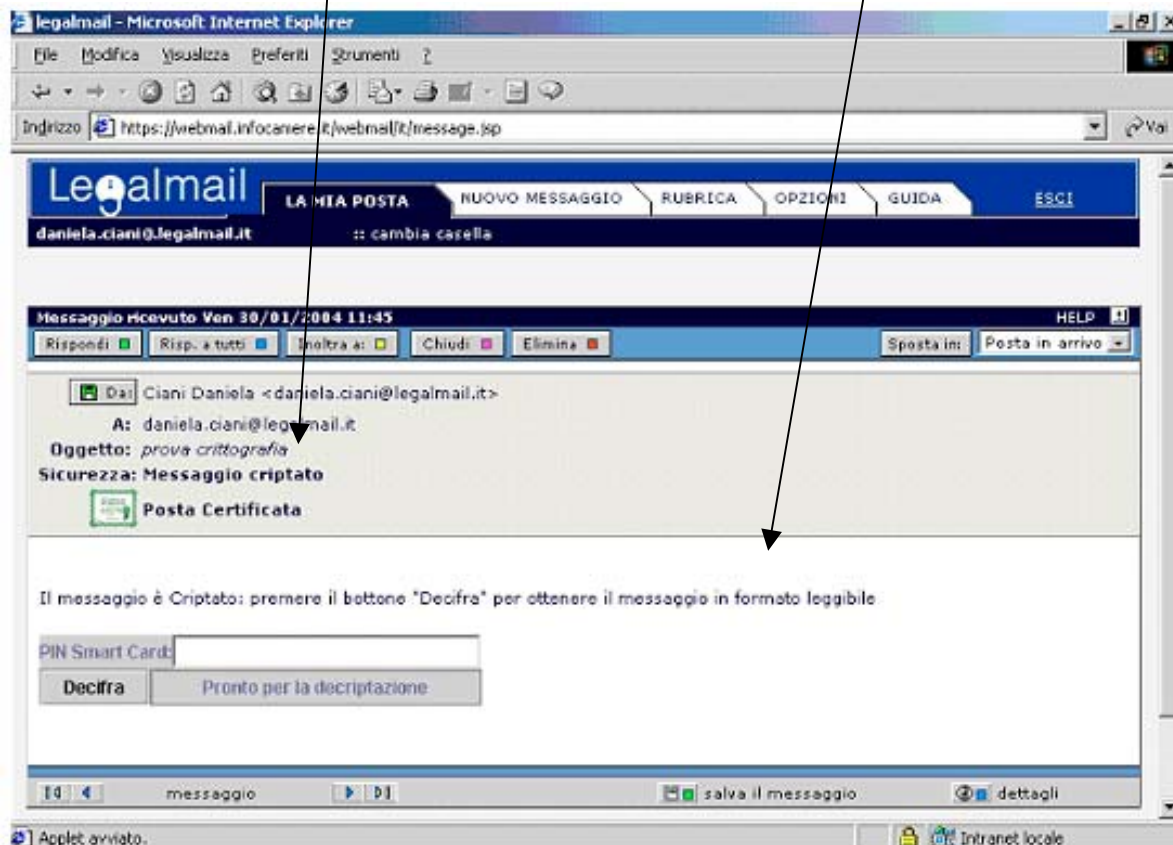
-  e  permette di aprire una “finestra” e di rispondere al mittente o a tutti i destinatari del messaggio compreso il mittente (cfr. [Nuovo Messaggio](#));
-  permette di aprire una “finestra” e di inviare ad altri destinatari il messaggio;
-  chiude la finestra e torna alla finestra precedente;
-  elimina il messaggio portandolo nella cartella Trash (se impostata);
-  posto accanto all’indirizzo e-mail del mittente, consente di inserire l’indirizzo nella rubrica (cfr. [Rubrica](#));
-  consente di spostare il messaggio nella cartella selezionata dalla box posta a destra.

In basso le frecce consentono di scorrere i messaggi.

-  **salva il messaggio:** consente di salvare il messaggio su disco
-  **versione stampabile:** consente di stampare il messaggio
-  **dettagli:** compare una finestra con i dettagli relativi al messaggio.

3.3.1 Ricezione di messaggi crittografati

Se l'utente riceve un messaggio crittografato, quando seleziona il messaggio per leggerlo, nella riga sicurezza troverà scritto **Messaggio crittato**. Inoltre, nella parte riservata al testo del messaggio, comparirà la scritta: " Il messaggio è crittato: premere il bottone decifra per ottenere il messaggio in formato leggibile". Il sistema propone quindi la maschera per digitare il pin.



Il sistema provvede a effettuare le verifiche e ad aprire il messaggio (anche nel caso l'utente stia consultando il messaggio di consegna di un messaggio da lui stesso crittografato).

3.4 Nuovo Messaggio

Dalla maschera principale selezionare la cartella Nuovo Messaggio.

A seconda della modalità selezionata, Normale o Avanzata (come indicato nella parte alta della maschera) è possibile utilizzare opzioni diverse della posta.

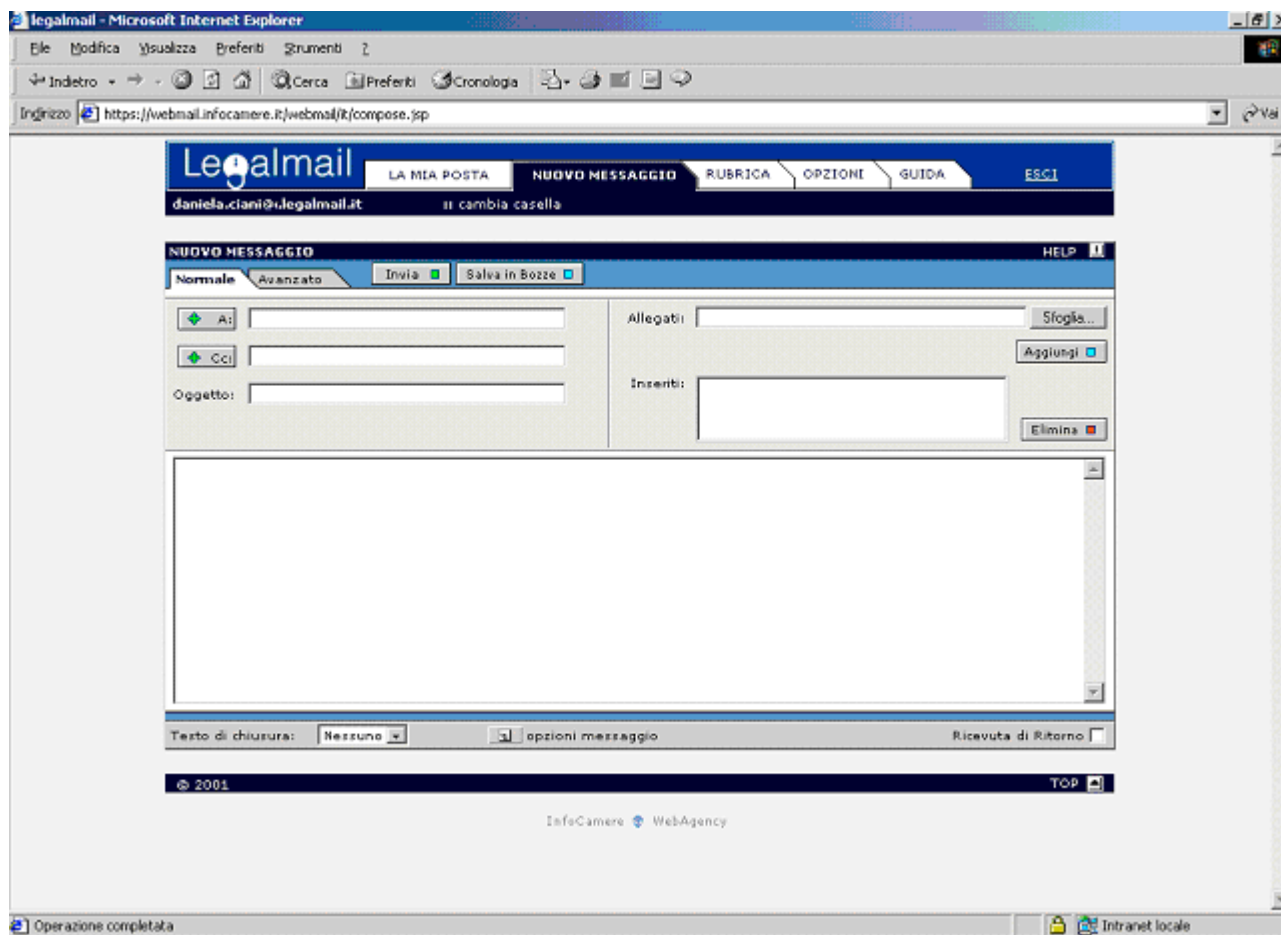
La modalità avanzata permette all'utente di utilizzare la firma digitale e la crittografia.

Per usufruire dei servizi di firma digitale e crittografia è necessario che l'utente abbia una smartcard InfoCamere e che abbia provveduto a scaricare alcuni MB di software sulla propria stazione di lavoro (cfr. [Accesso via Webmail](#)).

E' da tenere presente che la codifica "mime" degli allegati ai messaggi fa aumentare la dimensione del messaggio inviato. Questo significa che un messaggio con un allegato di 100KB potrebbe diventare durante la spedizione di 140 KB: di questo va tenuto conto nella valutazione dello spazio a disposizione nella casella quando si fanno molteplici invii in "TO" (per la ricevuta di consegna).







3.4.1 Modalità Normale

La finestra Nuovo Messaggio; nel caso si utilizzi la Modalità Normale; si presenta così:



La Modalità Normale permette di inviare messaggi di posta certificata senza firma e crittografia.

Esaminiamo i campi della videata:

-  Indirizzo del destinatario primario. Nel caso di più destinatari è necessario separare gli indirizzi e-mail con la virgola. E' possibile digitare gli indirizzi direttamente nel campo oppure selezionare gli indirizzi dalla rubrica personale cliccando sul bottone + **A** ; per questi destinatari la ricevuta di consegna conterrà copia del messaggio inviato. E' necessario che per ogni messaggio di posta certificata sia presente un destinatario primario (in "TO"). E' inoltre possibile usare il nome breve ("nickname") del destinatario inserito in rubrica.
-  Indirizzo del destinatario per conoscenza. Nel caso di più destinatari è necessario separare gli indirizzi e-mail con la virgola. E' possibile selezionare gli indirizzi dalla rubrica personale cliccando sul bottone. Non è consentito l'utilizzo del BCC con posta certificata;
- **Allegati:** il tasto **Sfoggia** permette di cercare e selezionare, attraverso la maschera della gestione risorse del pc., i documenti da allegare. Per allegare più di un documento, premere il tasto . Il documento sarà inserito in una nuova finestra (Inseriti) dove vengono elencati i documenti allegati. Il tasto  consente di togliere dall'elenco degli allegati da spedire il documento selezionato;
- **Oggetto:** oggetto del messaggio;
-  il tasto **Invia** consente di inviare il messaggio;
-  salva i messaggi nella cartella draft.

La finestra principale nella parte bassa della maschera permette di digitare il testo del messaggio da inviare.

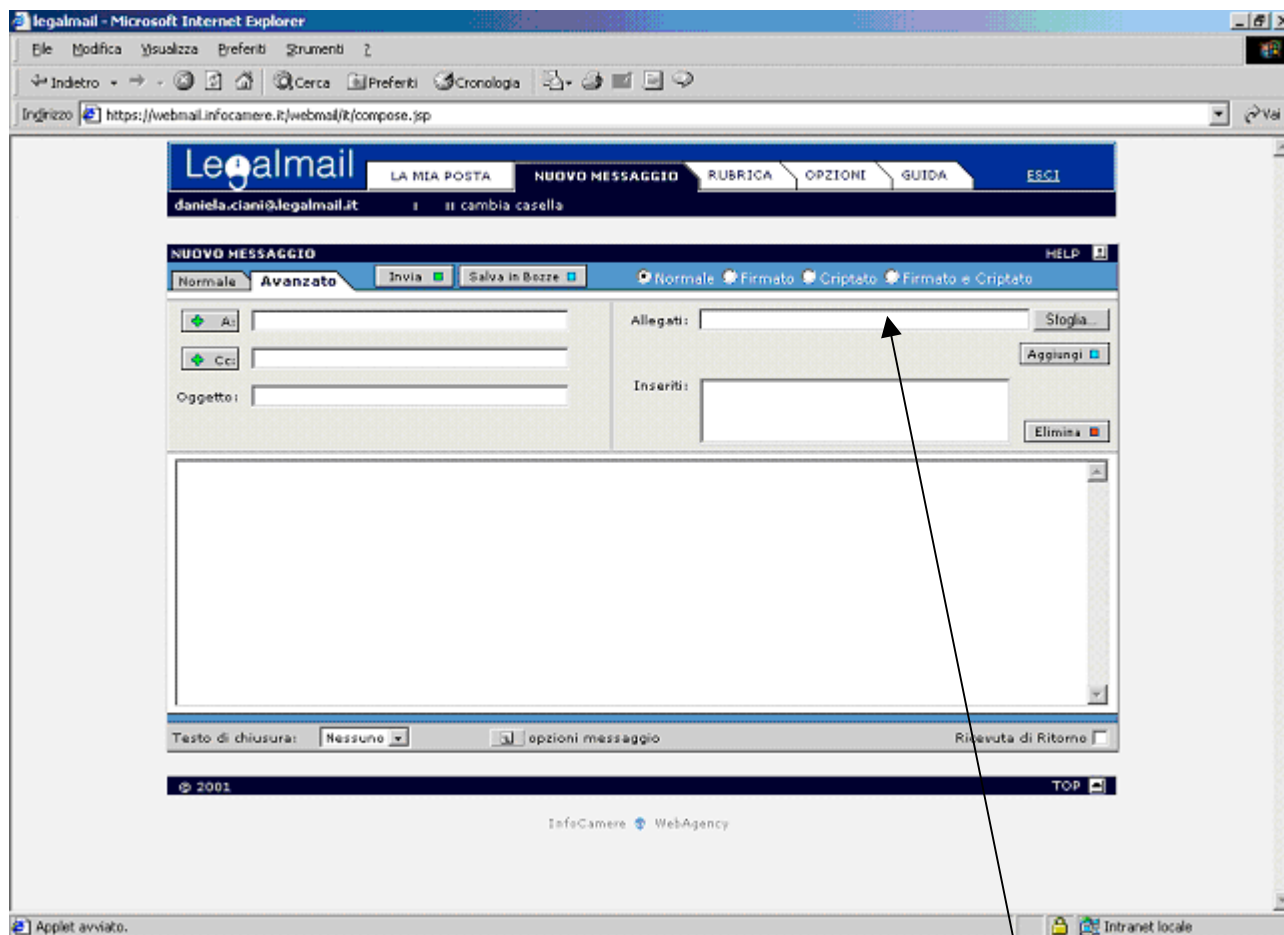
Il sistema chiederà una conferma per l'invio del messaggio qualora l'utente abbia settato l'opzione di salvataggio dei messaggi inviati (cfr. [Opzioni](#)) ed il messaggio in questione non possa essere salvato nella cartella per mancanza di spazio sufficiente nella casella.

3.4.2 Modalità avanzata

La Modalità avanzata permette di inviare messaggi di posta certificata utilizzando anche la firma digitale e la crittografia.

La finestra Nuovo Messaggio presenta gli stessi campi della Modalità normale e alcune opzioni specifiche della Modalità Avanzata.

La maschera della Modalità avanzata si presenta così:



I campi della maschera in modalità avanzata sono gli stessi della maschera della modalità normale.

La differenza tra le due maschere consiste nella possibilità di selezionare le voci per la crittografia e la firma digitale.

Sono presenti 4 possibili selezioni per tipologia di invio (cfr. [Note e particolarità dei messaggi di posta certificata](#)):

- **Normale:** il messaggio inviato è un messaggio di posta certificata (quindi firmato dal provider)
- **Firmato:** il messaggio inviato è un messaggio di posta certificata ma è firmato digitalmente oltre che dal provider anche dall'utente attraverso la propria SmartCard rilasciata da InfoCamere (utilizzando la chiave privata del proprio certificato di autenticazione).
- **Criptato:** il messaggio inviato è un messaggio di posta certificata (quindi firmato dal provider) criptato (per garantire maggiore riservatezza) con la chiave pubblica del certificato di autenticazione del destinatario

- **Firmato e Criptato:** il messaggio inviato è un messaggio di posta certificata che non solo risulta firmato sia dal provider che dall'utente (attraverso la propria SmartCard rilasciata da InfoCamere) ma anche criptato per garantire maggiore riservatezza.

Dopo avere premuto il tasto invia, Webmail provvede a spedire il messaggio e, se il messaggio è stato inviato con successo, il sistema riporta alla maschera della Mia Posta e compare in alto a sinistra la scritta "Messaggio inviato con successo".

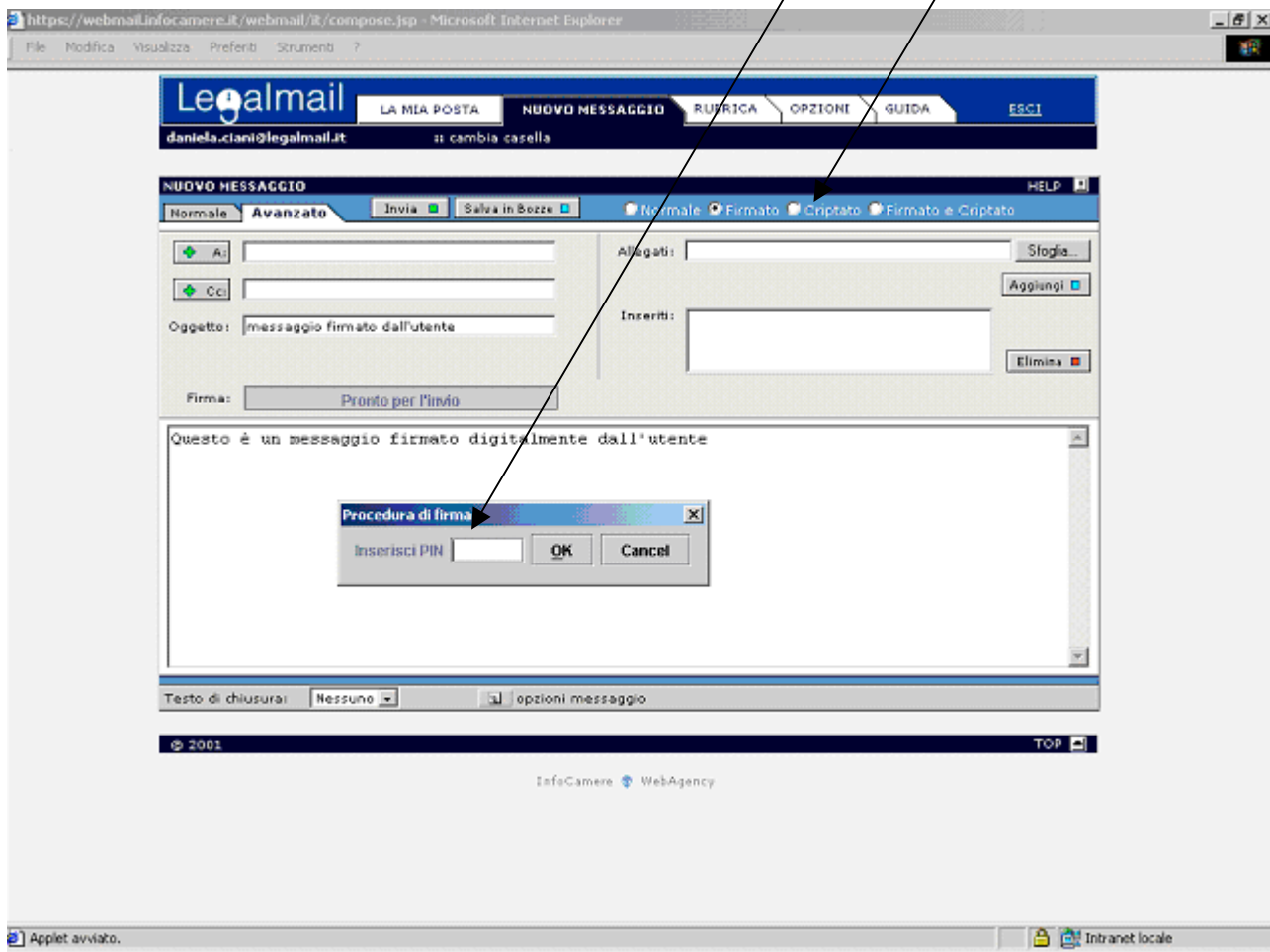
Messaggio firmato digitalmente e/o criptato

Per firmare e/o crittografare un messaggio, l'utente deve preparare il messaggio da inviare utilizzando la modalità avanzata.

L'utente deve indicare la tipologia di messaggio selezionando una delle voci: Normale, Firmato, Criptato, Firmato e Criptato.

Se l'utente vuole firmare digitalmente il messaggio, al momento dell'invio deve inserire la propria smartcard nel lettore: il sistema chiederà attraverso la maschera "Procedura di firma" di digitare il pin e premere il tasto **OK**.

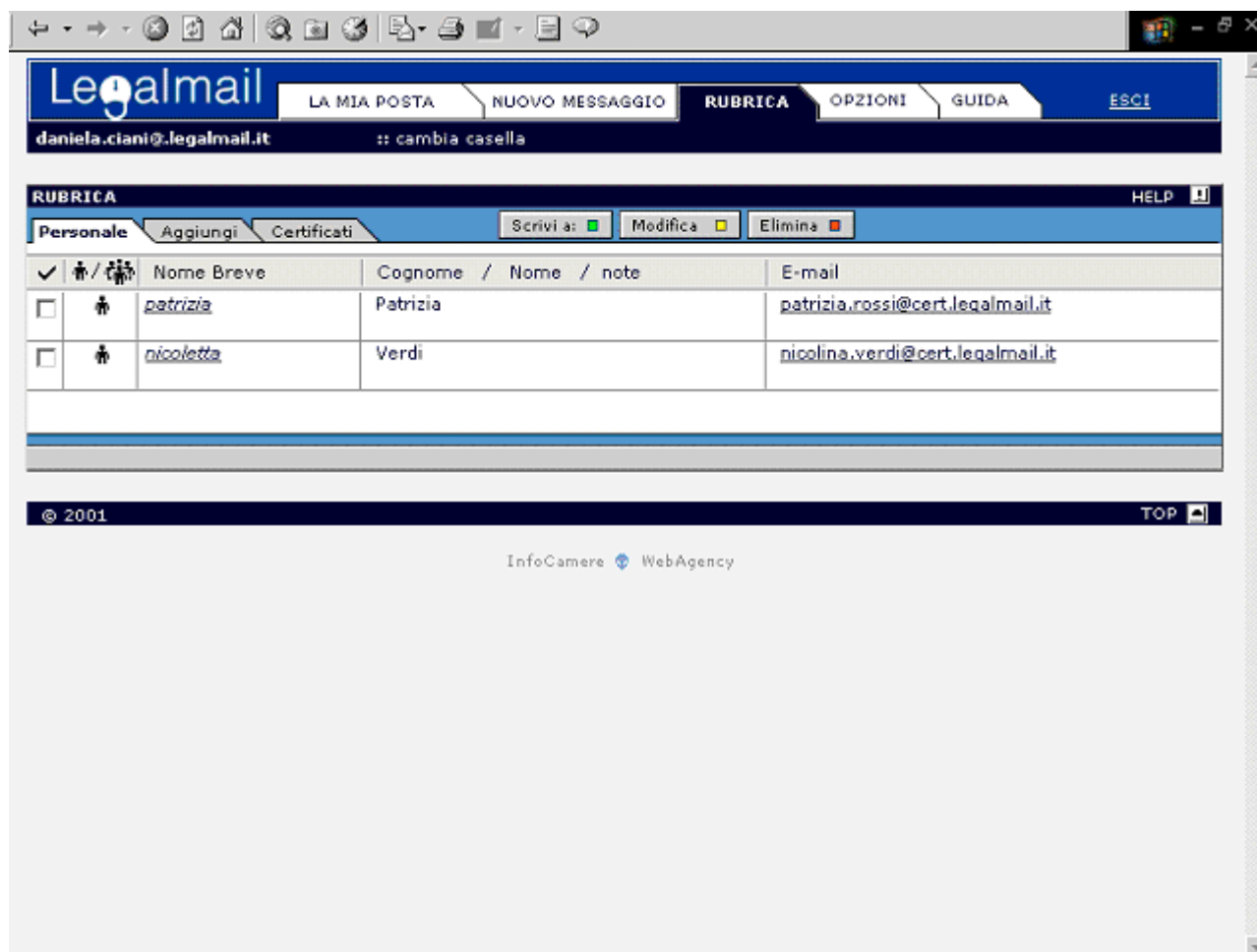
Se l'utente vuole crittografare il messaggio è necessario che mittente e destinatario abbiano un certificato riconosciuto da webmail. Se il mittente non ha il certificato del destinatario l'invio viene effettuato ma il mittente non potrà più leggere il messaggio inviato. Per conoscere il certificato del destinatario l'utente deve aver ricevuto un messaggio firmato digitalmente dal destinatario.



3.5 Rubrica

Ogni utente può creare una rubrica personale di indirizzi di posta elettronici, archiviando certificati digitali.

Nella maschera della rubrica, la cartella **Personale** permette di inserire, modificare e cancellare un indirizzo di posta; è inoltre possibile creare e gestire gruppi di indirizzi di posta.



Nella metà superiore della maschera, l'utente trova l'elenco degli indirizzi inseriti nella rubrica. I tasti consentono di modificare o cancellare l'indirizzo di posta selezionato (con un flag da inserire a sinistra dell'indirizzo).

Il tasto permette di accedere alla maschera *Nuovo messaggio* in cui è già inserito l'indirizzo precedentemente selezionato.

Inserimento di un indirizzo o di un gruppo di posta (cartella Aggiungi):

- per inserire un indirizzo di posta nella rubrica, l'utente deve compilare i campi **Nome Breve (Nickname)**, **Cognome e Nome**, **E-mail**
- per creare un gruppo di posta, l'utente deve compilare il campo **Nome Gruppo** e selezionare gli indirizzi della rubrica da inserire nel gruppo (attraverso il tasto freccia destra). E' possibile inserire nel gruppo anche indirizzi non presenti in rubrica attraverso l'apposito campo.

Premere il tasto **Aggiungi** per inserire l'indirizzo nella rubrica o creare il gruppo.

The screenshot displays the Legalmail web interface. At the top, there is a navigation bar with the Legalmail logo and several menu items: 'LA MIA POSTA', 'NUOVO MESSAGGIO', 'RUBRICA', 'OPZIONI', 'GUIDA', and 'ESCI'. Below this, the user's email address 'daniela.ciani@legalmail.it' is shown. The main content area is titled 'RUBRICA' and has a sub-header with 'PERSONALE', 'AGGIUNGI', and 'CERTIFICATI' tabs. The 'AGGIUNGI' tab is selected, and there are 'AGGIUNGI' and 'ANNULLA' buttons. The interface is divided into two main sections: 'Aggiungi Nuovo Contatto' and 'Aggiungi Nuovo Gruppo'. The 'Aggiungi Nuovo Contatto' section includes input fields for 'Nome Breve', 'Cognome Nome', and 'E-mail', along with a 'Note' field. The 'Aggiungi Nuovo Gruppo' section includes a 'Nome Gruppo' field, a list of contacts from the address book (e.g., nicolina.verdi@cert.legalmail.it, patrizia.rossi@cert.legalmail.it) with a right arrow button to add them to the group, and a field for 'Indirizzi inseriti nel gruppo'. There is also a field for 'Inserisci indirizzo non in rubrica' and a 'Note' field. The footer shows '© 2001' and 'TOP'.

Attenzione: i messaggi ricevuti da posta certificata, malgrado le apparenze, non sono spediti dal mittente originale ma dal suo provider di posta certificata. In certe operazioni particolari si deve tener conto di questa caratteristica. Per esempio: se si intende aggiungere il mittente alla propria rubrica, l'operazione va effettuata dalla maschera dove è contenuto il testo. Altrimenti, malgrado l'intestazione del nome in rubrica sembri corretta, l'indirizzo inserito in rubrica non lo sarà: verrà inserito l'indirizzo del provider del mittente e i messaggi spediti non arriveranno mai alla giusta destinazione.

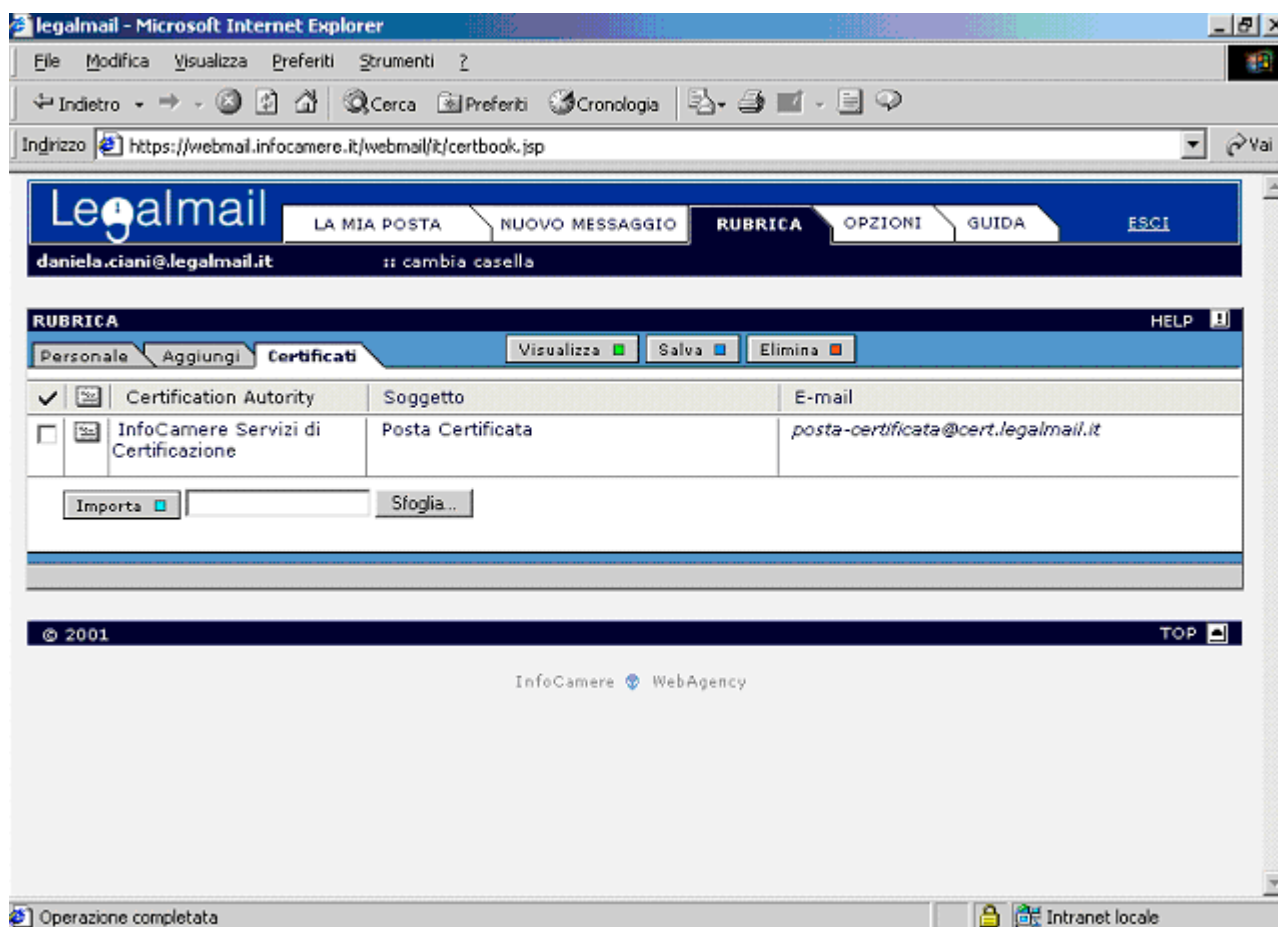
In fase di composizione del messaggio per inserire l'indirizzo e-mail nell'apposito campo è possibile: 1) digitare l'indirizzo, 2) reperirlo dalla rubrica, 3) digitare il nome breve ("nickname") dell'indirizzo memorizzato in rubrica.






Rubrica (cartella **Certificati**)

Attraverso la finestra **Certificati** è possibile archiviare i certificati di firma digitale quando vengono ricevuti messaggi di posta elettronica firmati digitalmente.

Si ricorda che quando l'utente riceve messaggi di posta certificata da un altro sistema (diverso da Legalmail) è necessario (solo la prima volta) "trustare" il certificato di firma del provider mittente: è cioè necessario far riconoscere al sistema la validità del certificato di firma (come descritto più avanti).

Inoltre, per inviare un messaggio crittografato è necessario aver scaricato e archiviato il certificato digitale dell'utente destinatario (nel caso questi abbia un certificato rilasciato da un ente certificatore diverso da InfoCamere): per fare questo, l'utente deve aver prima ricevuto un messaggio firmato digitalmente dall'utente che sarà destinatario del messaggio crittografato.



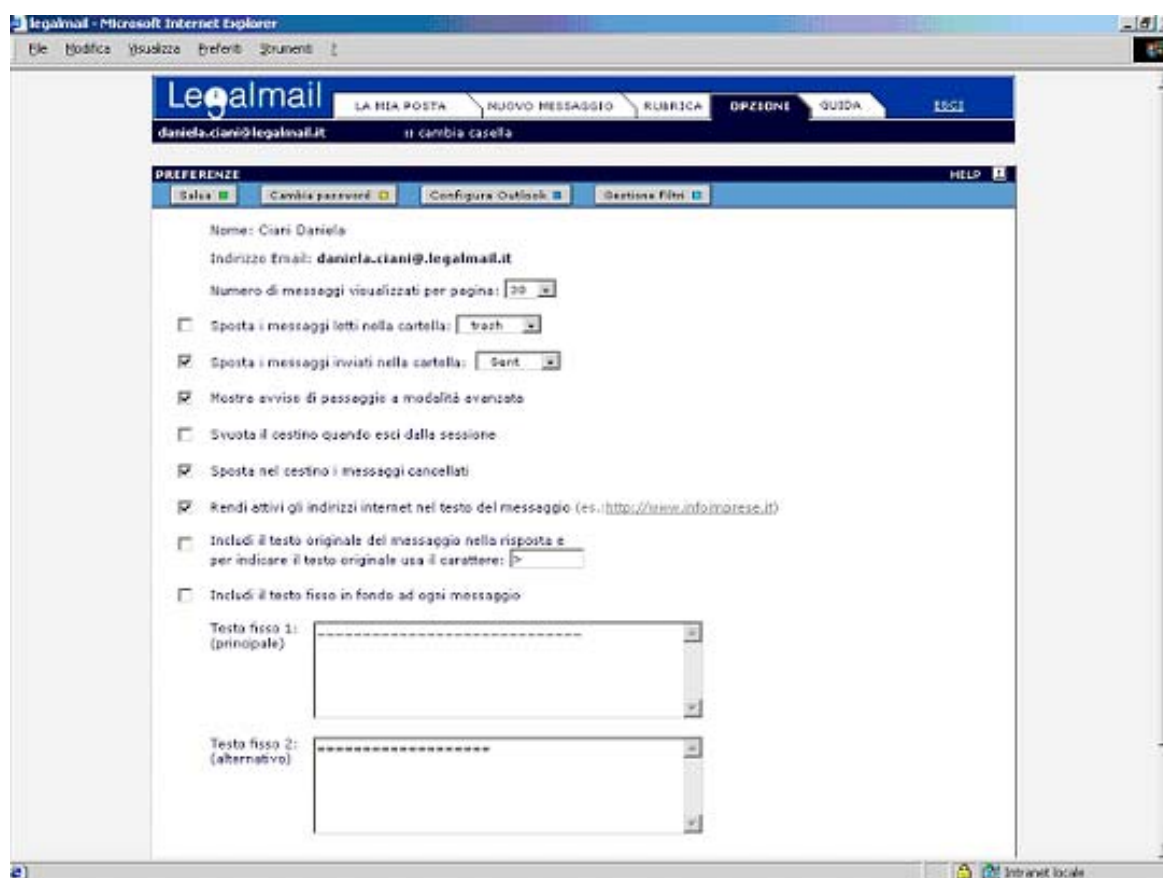
- **Visualizza**  permette di visualizzare i contenuti del certificato (Soggetto, Emittente, Validità e Proprietà del certificato);
- **Salva**  consente il salvataggio del certificato su di un disco locale;
- **Elimina**  permette l'eliminazione dei certificati selezionati;
- **Importa**  importare dal disco locale un certificato digitale attraverso le seguenti operazioni: prima cliccare su "Sfoglia...", individuare il file "nome.cer" e quindi cliccare su "Apri"; sarà visualizzato il percorso del certificato, cliccare quindi sul pulsante **Importa** 

L'importazione dei certificati può avvenire anche attraverso l'apposita opzione dal messaggio di posta ricevuto (vedi paragrafo)

In aggiunta alla Rubrica Personale possono essere presenti, se attivate, una o più Rubriche Esterne (LDAP). In questo caso l'utente avrà a disposizione un'altra cartella "Esterna" dove potrà accedere alla funzione di ricerca indirizzo.


3.6 Opzioni

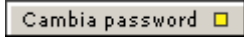
La maschera delle Opzioni serve per configurare/personalizzare Webmail: è possibile compilare i testi fissi da inserire su ogni messaggio e indicare dove archiviare i messaggi inviati, letti ecc...





Note:

- l'opzione "Sposta messaggi nella cartella XXX", se abilitata, permette di mantenere copia dei messaggi inviati in una cartella a scelta tra quelle disponibili (XXX). Se si toglie la selezione da questa opzione, i messaggi inviati non saranno consultabili.
- l'opzione "Sposta nel cestino i messaggi cancellati" permette di cancellare i messaggi senza passare per il cestino (i messaggi cancellati non passando dal cestino non saranno più recuperabili); questa opzione può essere utilizzata qualora la casella fosse talmente piena da impedire all'utente di cancellare i messaggi.
- L'opzione "Mostra avviso di passaggio a modalità avanzata" consente di visualizzare o meno l'avviso del passaggio alla modalità avanzata.

Il tasto  permette di acquisire le modifiche effettuate.

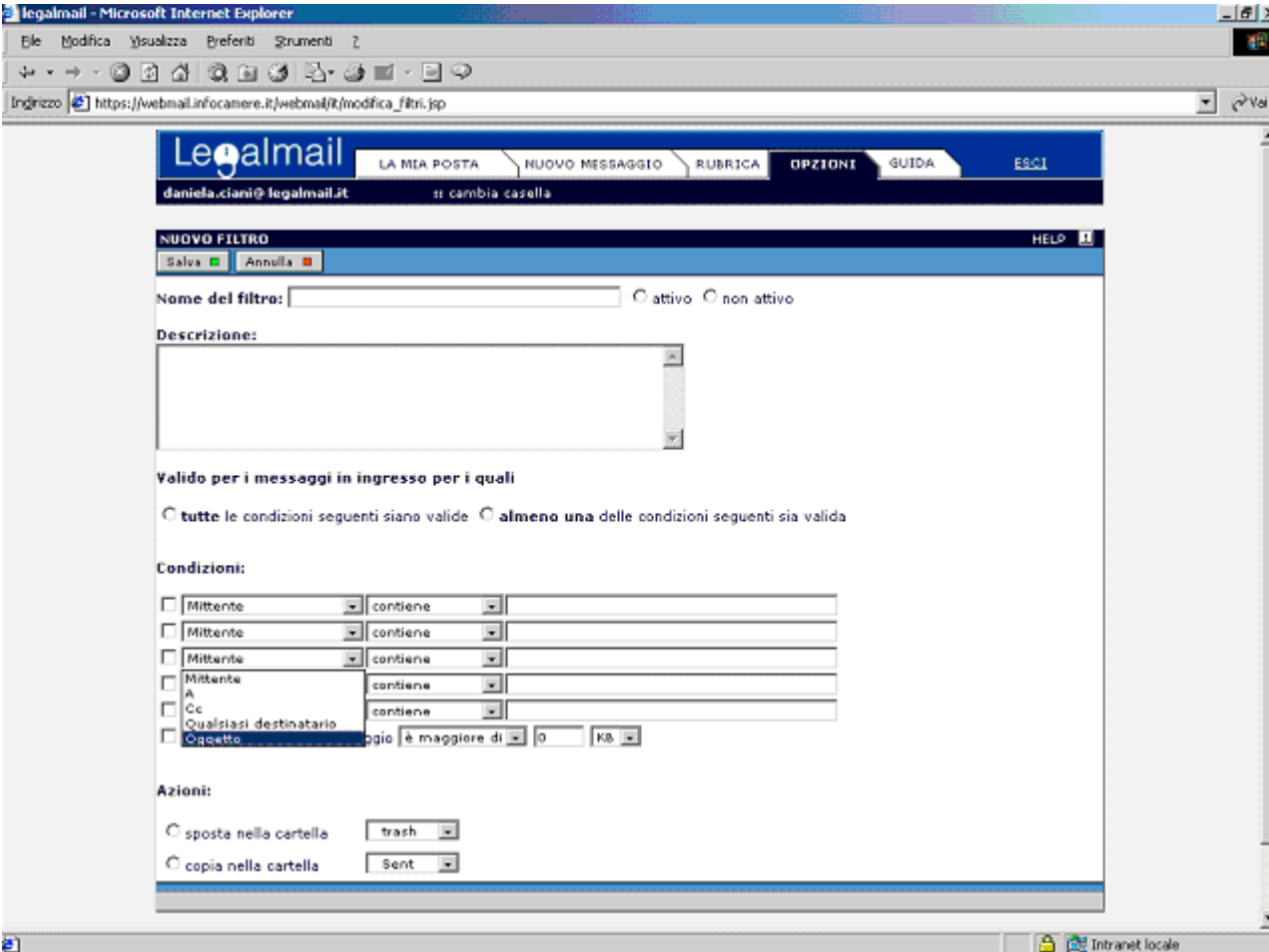
Il tasto  permette di modificare la propria password in qualsiasi momento (è consigliabile effettuare il cambio password almeno alla prima attivazione del servizio).

Il tasto  consente di utilizzare un configuratore automatico per Outlook/Outlook Express. Il configuratore predispose in Outlook / Outlook Express una configurazione standard della stessa casella che si sta usando con Webmail. E' utilizzabile con versioni abbastanza recenti dei due prodotti eccetto Outlook 2002.

Il tasto  consente di impostare, in webmail, dei filtri a livello di casella. I filtri consentono di reindirizzare automaticamente in alcune cartelle (su server) i messaggi che hanno le caratteristiche impostate dall'utente. I filtri hanno effetto su tutti i messaggi, indipendentemente dal fatto che poi l'utente utilizzi webmail o un client (es. Outlook) per consultarli.

E' però sconsigliato settare filtri per cancellare in automatico messaggi ricevuti (che soddisfano a certe caratteristiche) data la tipologia di casella ("ufficiale") utilizzata.

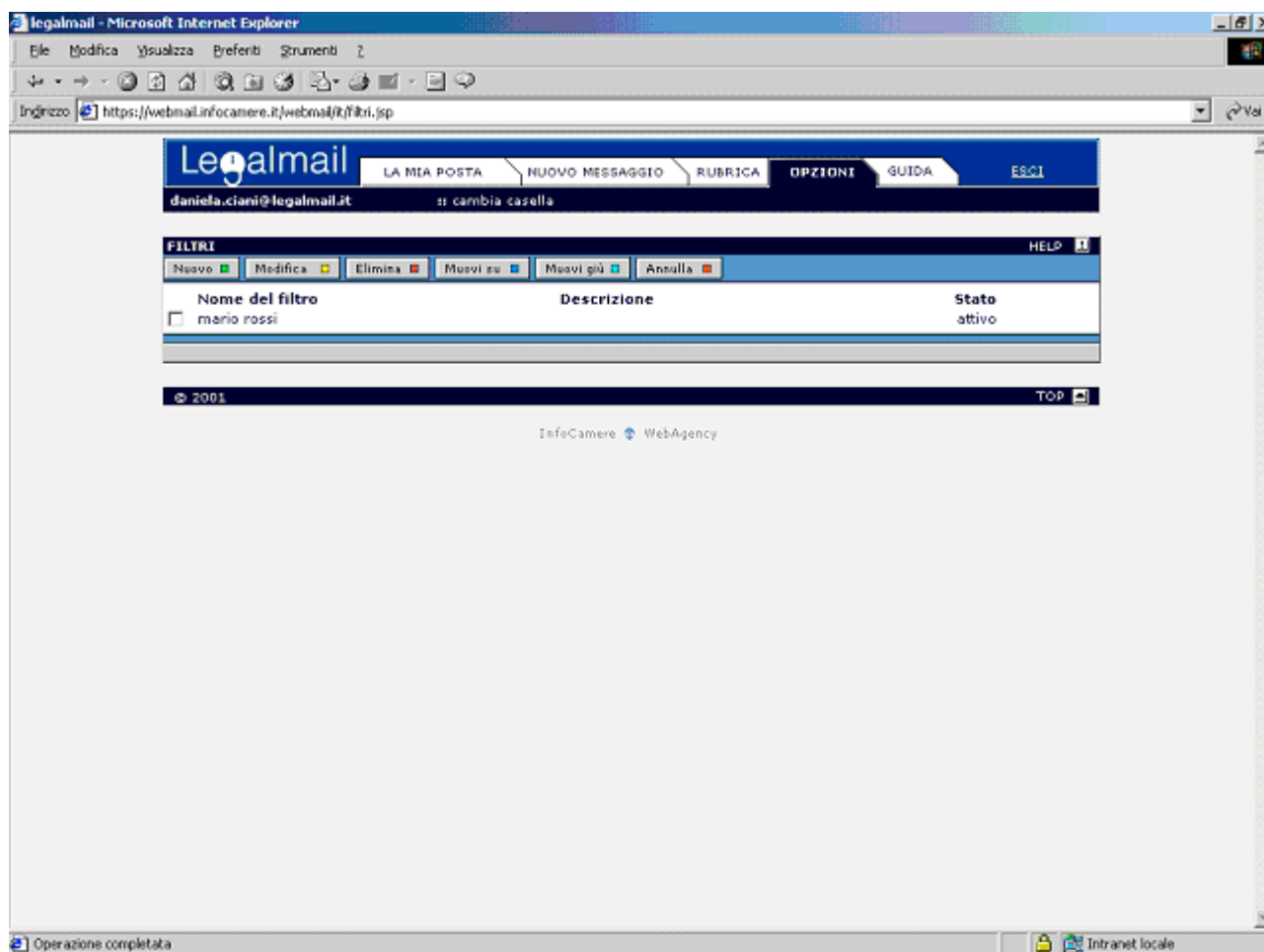
Per inserire un filtro è necessario premere il bottone "Gestione Filtri" del menù Opzioni e successivamente premere il bottone "Nuovo": compare la seguente maschera.



Per impostare il filtro l'utente deve:

- indicare il nome del filtro;
- impostare il filtro utilizzando la sezione “condizioni”(con l’aiuto degli appositi menù a tendina);
- indicare se le condizioni impostate devono essere tutte soddisfatte o se almeno una delle condizioni deve essere soddisfatta;
- indicare l’Azione (se spostare o copiare in una cartella il messaggio che soddisfa il filtro);
- rendere attivo il filtro.

Quando l’utente ha impostato uno o più filtri la maschera che si presenta premendo il bottone “Gestione Filtri” diventa:



Attraverso questa maschera è possibile anche selezionare un filtro per visualizzarlo o modificarlo.

3.7 Guida

La cartella Guida permette di consultare la guida in linea di Webmail



4. Esempi di messaggi di posta certificata

Nei successivi paragrafi sono riportati alcuni esempi di messaggi di posta certificata: gli esempi si riferiscono a Webmail. Se l'utente utilizza un client di posta elettronica per accedere alla posta certificata otterrà messaggi simili a quelli illustrati di seguito (a cambiare sarà solo la forma grafica).

Nota:

alcuni client di posta aprono in automatico certe tipologie di allegati; per questo motivo l'utente potrà non trovare alcuni degli allegati descritti nei paragrafi successivi. Per esempio alcuni client aprono automaticamente l'allegato postacert.eml: il testo dell'allegato viene "attaccato" di seguito alla "busta" di posta certificata.

Inoltre alcuni client propongono gli allegati con estensione eml con il nome dell'oggetto e non con il nome del file.

4.1 Ricevuta di Accettazione

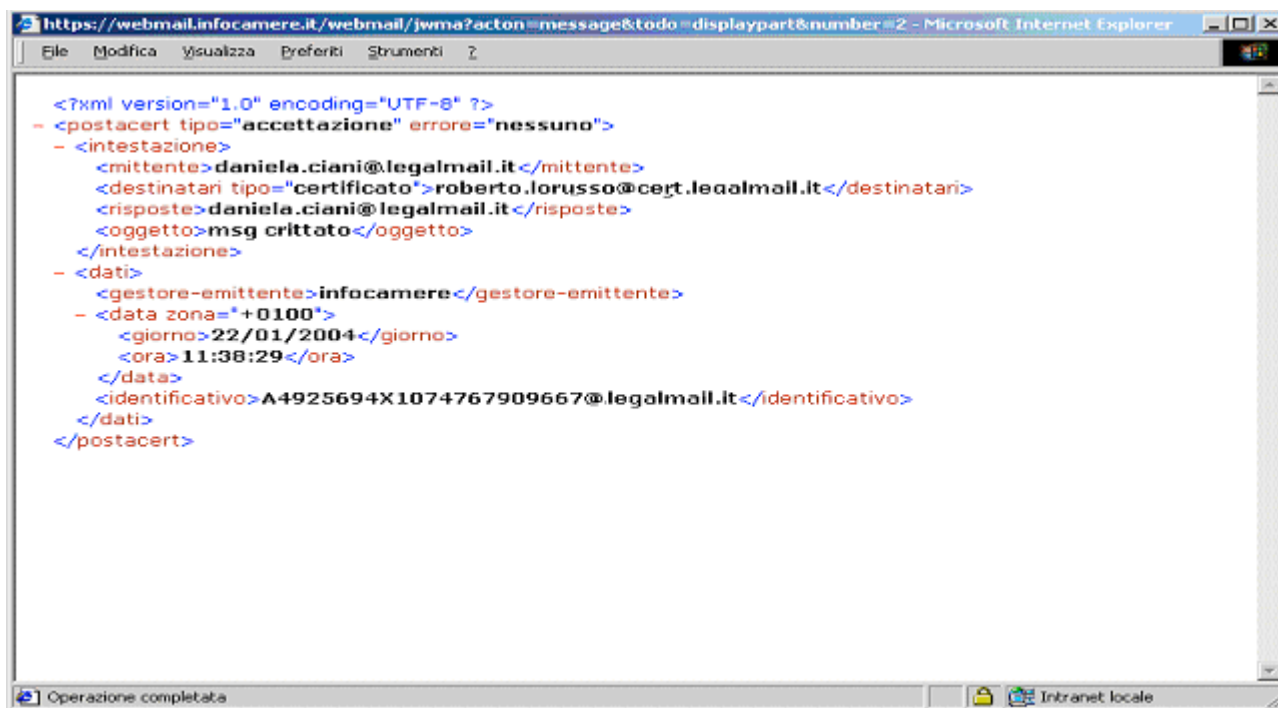
Il messaggio di accettazione inviato dal gestore del mittente è composto di 3 parti:

- Dati del messaggio
- Ricevuta di accettazione
- Informazioni di dettaglio



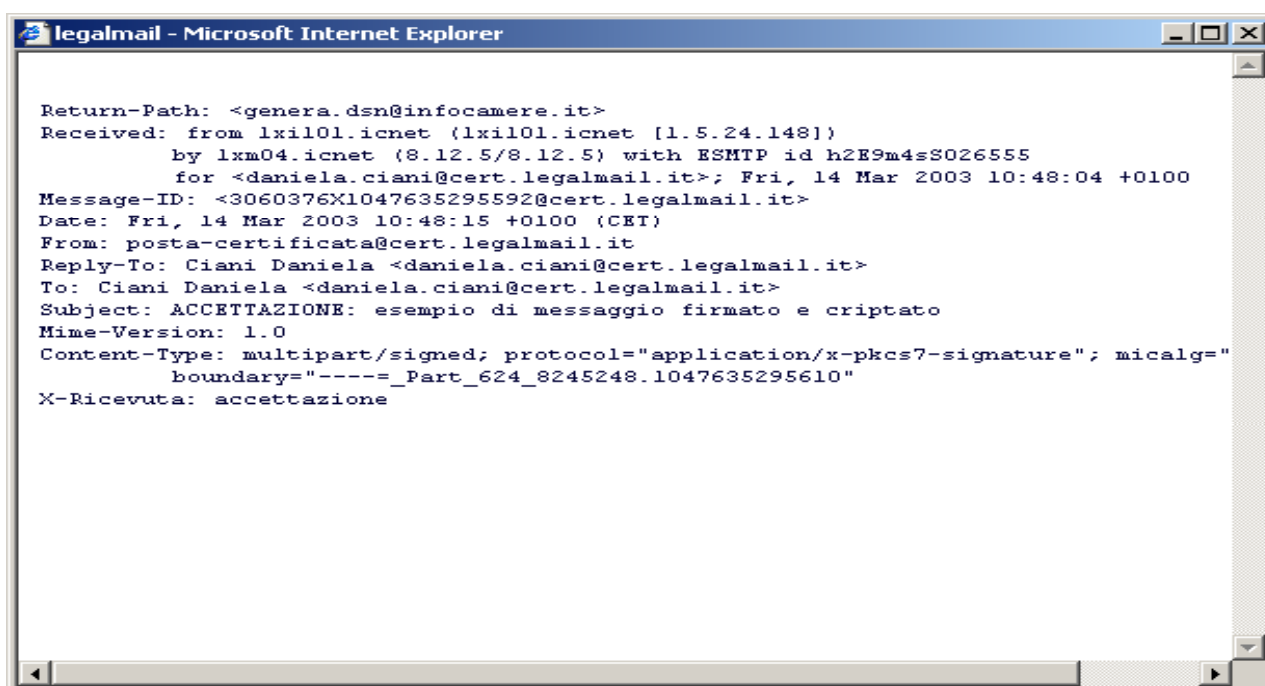
La prima parte contiene le informazioni del mittente, altri destinatari, oggetto, la possibilità di verificare la firma (botone "Sicurezza") e i bottoni per la gestione del messaggio ("Rispondi", "Inoltra a", "Chiudi", "Elimina" ecc...)

Per ciascun messaggio di accettazione di posta certificata è allegato il file Daticert.xml contenente i dati di certificazione (vedi es. sotto)



```
<?xml version="1.0" encoding="UTF-8" ?>
- <postacert tipo="accettazione" errore="nessuno">
- <intestazione>
  <mittente>daniela.ciani@legalmail.it</mittente>
  <destinatari tipo="certificato">roberto.lorusso@cert.legalmail.it</destinatari>
  <risposte>daniela.ciani@legalmail.it</risposte>
  <oggetto>msg crittato</oggetto>
</intestazione>
- <dati>
  <gestore-emittente>infocamere</gestore-emittente>
  - <data zona="+0100">
    <giorno>22/01/2004</giorno>
    <ora>11:38:29</ora>
  </data>
  <identificativo>A4925694X1074767909667@legalmail.it</identificativo>
</dati>
</postacert>
```

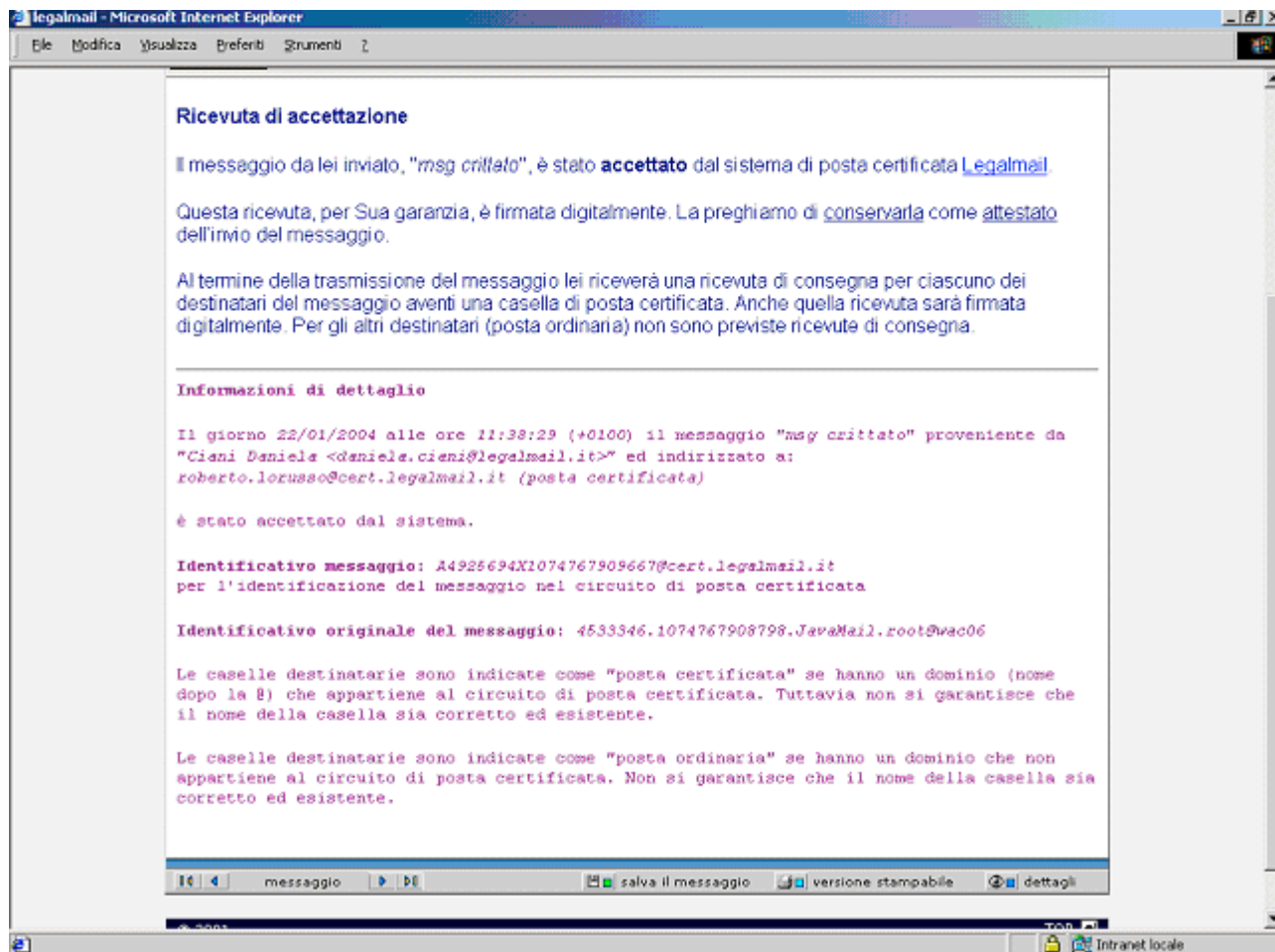
Il bottone "dettagli" (in basso a destra) consente di accedere alle informazioni sulla spedizione del messaggio



```
Return-Path: <genera.dsn@infocamere.it>
Received: from lxi101.icnet (lxi101.icnet [1.5.24.148])
  by lxm04.icnet (8.12.5/8.12.5) with ESMTTP id h2E9m4sS026555
  for <daniela.ciani@cert.legalmail.it>; Fri, 14 Mar 2003 10:48:04 +0100
Message-ID: <3060376X1047635295592@cert.legalmail.it>
Date: Fri, 14 Mar 2003 10:48:15 +0100 (CET)
From: posta-certificata@cert.legalmail.it
Reply-To: Ciani Daniela <daniela.ciani@cert.legalmail.it>
To: Ciani Daniela <daniela.ciani@cert.legalmail.it>
Subject: ACCETTAZIONE: esempio di messaggio firmato e criptato
Mime-Version: 1.0
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg="
  boundary="-----_Part_624_8245248.1047635295610"
X-Ricevuta: accettazione
```

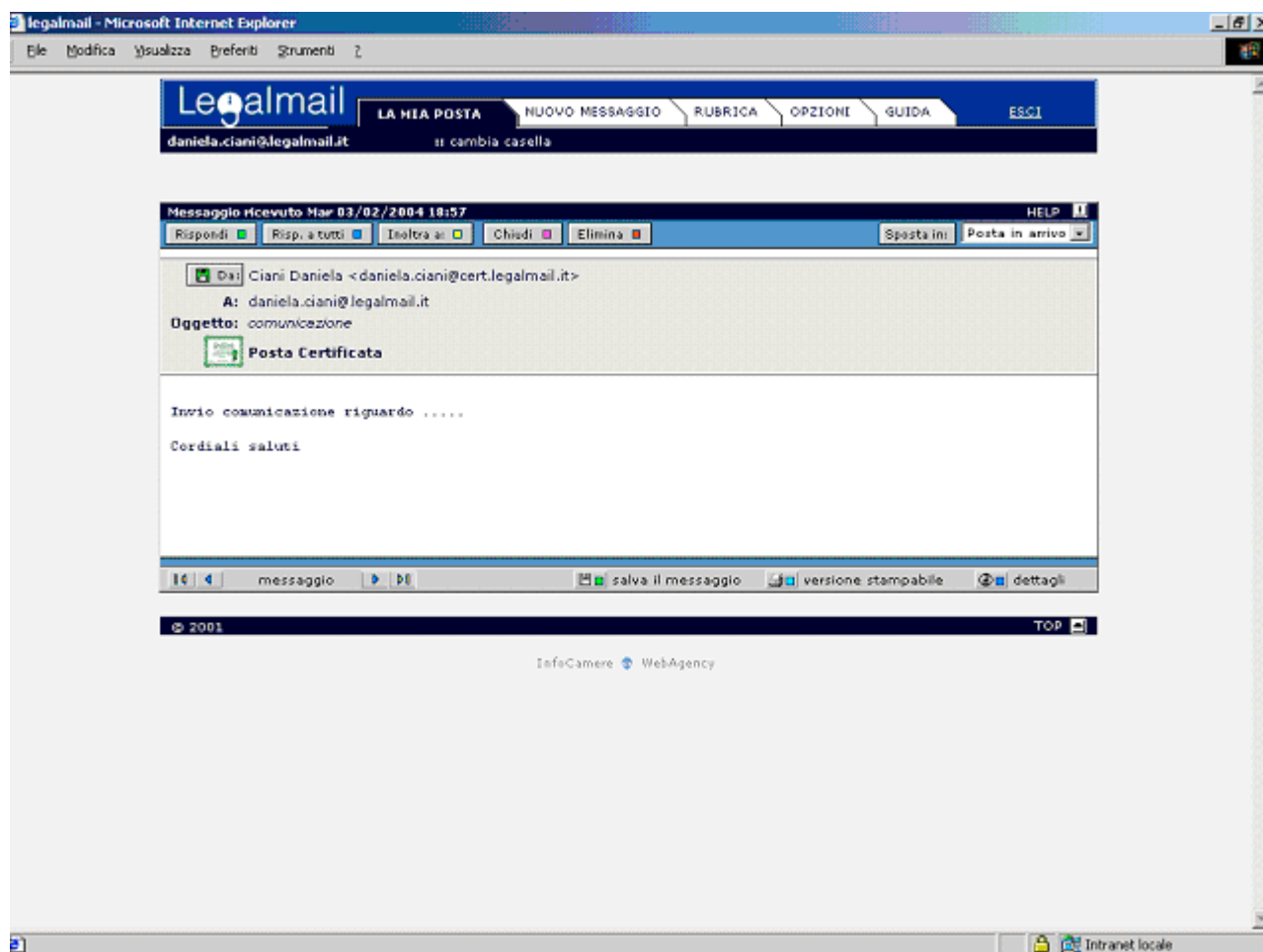

La seconda parte (Ricevuta di accettazione) contiene alcune informazioni sulla posta certificata e sul significato/valore delle ricevute.


La terza parte (Informazioni di dettaglio) riporta informazioni dettagliate sul messaggio (data e ora di invio, mittente, destinatario ecc..) come è possibile vedere nella seguente maschera:



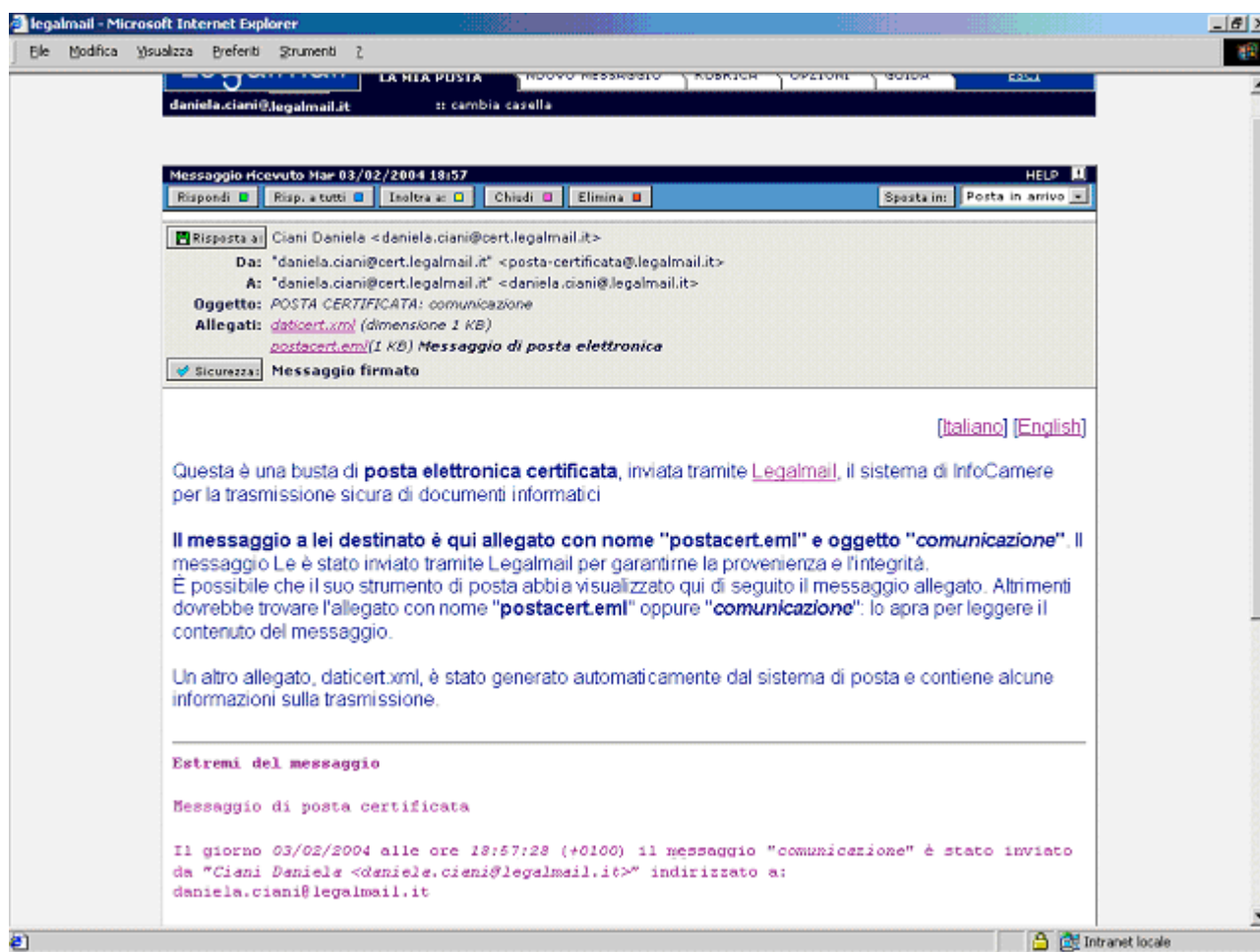
4.2 Messaggio di Posta Certificata

E' il messaggio che l'utente destinatario riceve da un altro utente con casella di posta certificata: appare subito il messaggio originale e solo a richiesta viene visualizzata la busta (messaggio di trasporto). Per i messaggi crittografati consultare l'apposito paragrafo.



Premendo il bottone  è possibile visualizzare la busta. La maschera che appare è composta di 3 parti

- Dati del messaggio (cfr. [Ricevuta di Accettazione](#)) dove sono presenti 2 file allegati: daticert.xml (contenente i dati di certificazione del messaggio) e postacert.eml dove è stato "imbustato" l'intero messaggio del mittente con gli eventuali documenti allegati del mittente (vedi esempio nella pagina seguente)
- Descrizione del messaggio (descrizione standard che informa l'utente sulle caratteristiche del messaggio ricevuto)
- Estremi del messaggio (contiene le informazioni su data e ora di spedizione, mittente e identificativo del messaggio)



Se il messaggio è stato crittografato occorre utilizzare la modalità avanzata: se l'utente sta utilizzando la modalità normale un messaggio lo avvisa (cfr. [Ricezione di messaggi crittografati](#))

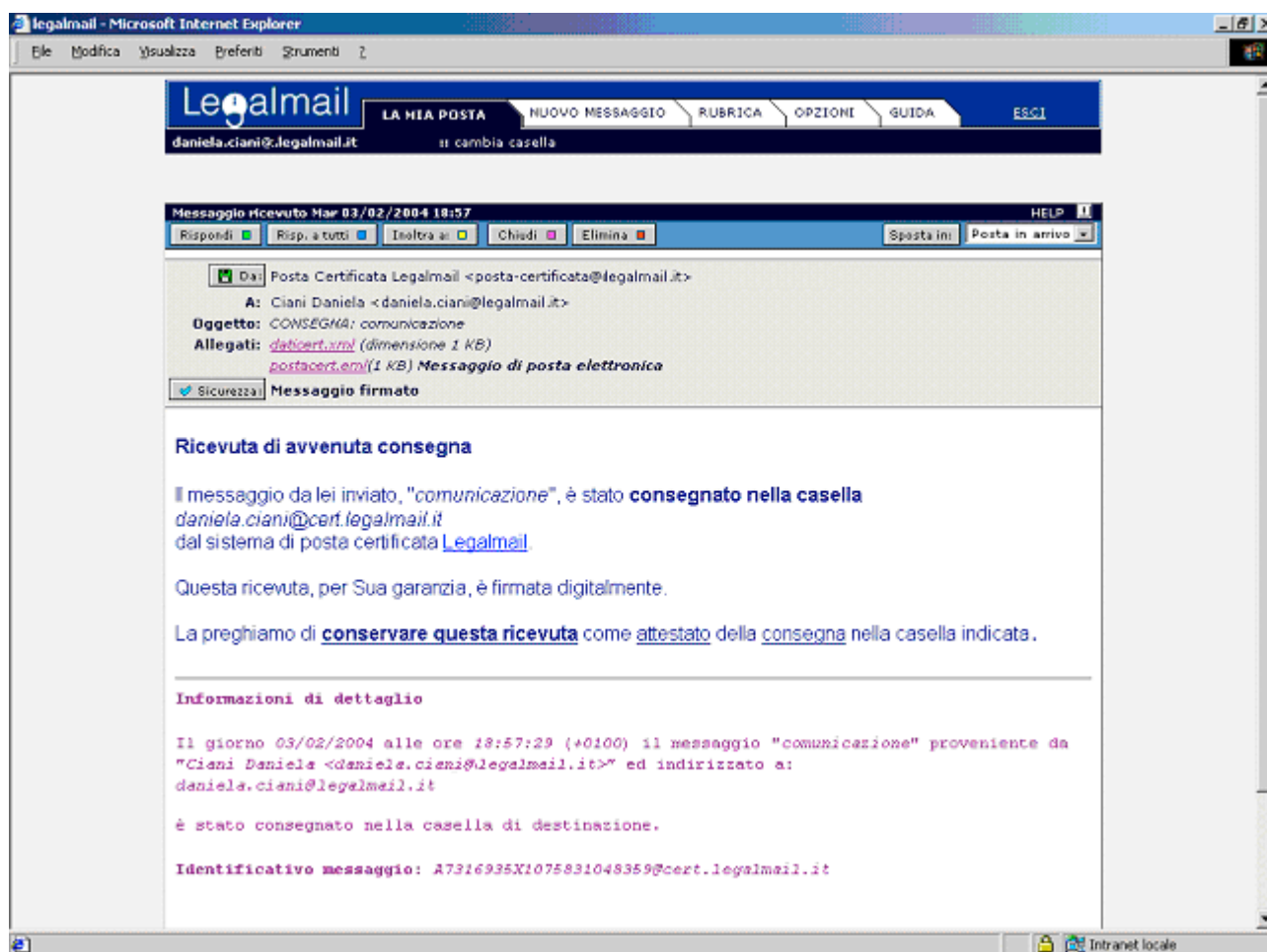
4.3 Ricevuta di Consegna

E' il messaggio inviato dal gestore di posta certificata del destinatario: contiene le informazioni che certificano l'avvenuta consegna nella casella di posta certificata del destinatario ed il messaggio originale inviato dal mittente (per i destinatari in TO).

Il messaggio è composto da :

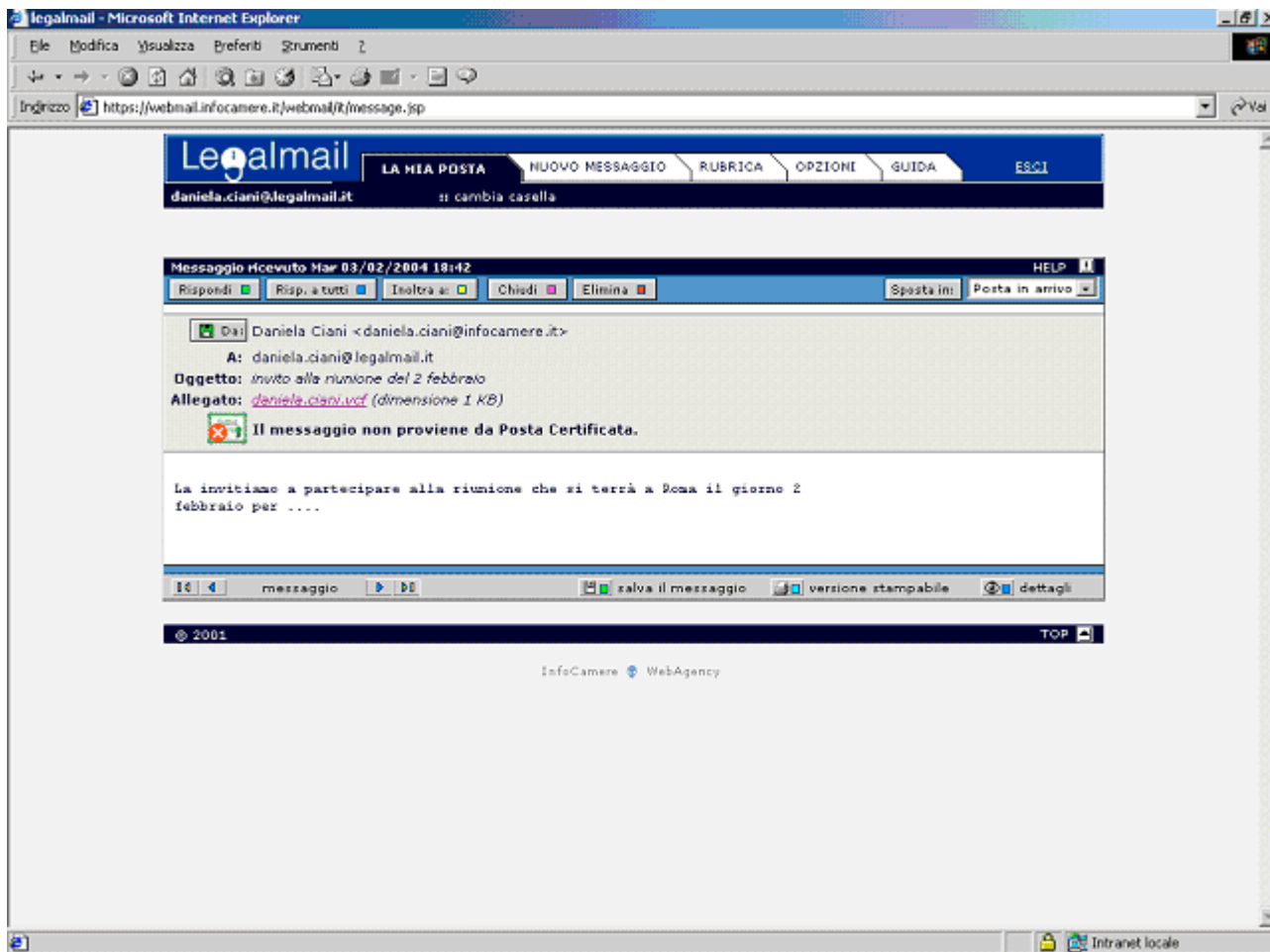
- Dati del messaggio (cfr. [Ricevuta di Accettazione](#); alla voce allegati sono presenti i 2 file: daticert.xml (contenente i dati di certificazione del messaggio) e postacert.eml dove è stato "imbustato" l'intero messaggio del mittente con gli eventuali documenti allegati del mittente (cfr. [Messaggio di Posta Certificata](#))
- Ricevuta di avvenuta consegna (questa parte del messaggio informa sull'avvenuta consegna del messaggio nella casella di posta destinataria e sul significato di questa ricevuta)
- Informazioni di dettaglio (contiene le informazioni su data e ora di spedizione, mittente e identificativo del messaggio)

Si ricorda che, se il messaggio è stato crittografato, occorre utilizzare la modalità avanzata (cfr. [Ricezione di messaggi crittografati](#)).



4.4 Anomalia di messaggio

Nel caso l'utente riceva un messaggio da una casella di posta non certificata il sistema identifica il messaggio con la scritta *Anomalia di messaggio* e provvede a indicare che il messaggio non proviene da Posta Certificata:



5. Requisiti Tecnici e Configurazione Client / Browser

5.1 Requisiti tecnici

La postazione dell'utente dovrà essere già dotata di:

- accesso a internet che permetta il colloquio attraverso i seguenti protocolli, elencati con le relative porte standard:
 - SMTPS 465** per spedire messaggi (via SMTP + SSL) con client di posta (consigliata)
 - SMTP 25** per spedire messaggi (via SMTP START-TLS) con client di posta
 - IMAP-S 993** per ricevere messaggi (via IMAP + SSL) con client di posta
 - POP3-S 995** per ricevere messaggi (via POP3 + SSL) con client di posta
 - HTTP 80** per accedere al sito www.legalmail.it contenente informazioni sul servizio
 - HTTPS 443** per utilizzare webmail come strumento di invio e lettura dei messaggi

- client di posta elettronica e/o un browser Internet a seconda di come l'utente preferisce accedere alla casella di posta. Per il client, utilizzabile via POP3 e IMAP, è necessario come versione minima: Outlook 5.50, o prodotti equivalenti/superiori. Per il browser, via https protocollo sicuro, per utilizzare le funzionalità complete di firma e crittografia è necessario come versione minima: Explorer 5.50, o prodotti equivalenti/superiori.

Per accedere al servizio Legalmail occorrono:

- user - id e password assegnate da InfoCamere con apposito profilo di abilitazione al servizio di posta.

Per firmare digitalmente i messaggi di posta occorre:

- certificato di autenticazione, rilasciato dall'Ente Certificatore InfoCamere nel caso l'utente utilizzi webmail via browser (in ambiente windows):
- certificato di autenticazione, rilasciato da un Ente Certificatore (per esempio InfoCamere) nel caso l'utente utilizzi il client per l'accesso alla casella di posta.

Il certificato di autenticazione deve contenere il nome della casella e-mail di posta certificata utilizzata (se il nome della casella fosse diverso non sarebbe possibile firmare correttamente).

Lo stesso certificato serve anche per inviare e ricevere messaggi crittografati e può essere utilizzato come alternativa a user - id e password per accedere al servizio webmail. Per utilizzare il certificato di autenticazione nel client e nel browser è necessario importarlo in questi strumenti secondo le procedure indicate nel sito www.card.infocamere.it

Per firmare digitalmente i documenti informatici occorre:

- certificato di sottoscrizione a norma dell’Agenzia per l’Innovazione (A.I.P.A.) rilasciato dall’Ente Certificatore (es. InfoCamere) con il relativo dispositivo di firma
- **DìKe**, il software InfoCamere per firmare digitalmente i documenti (download gratuito dal sito www.card.infocamere.it/software) nel caso si utilizzi un certificato InfoCamere oppure altri strumenti di firma nel caso si utilizzi altro certificato.

Il sistema di posta certificata Legalmail consente di custodire la posta in ambiente protetto: il sistema è dotato di più livelli di firewall, intrusion detection, antivirus per i messaggi in entrata ed in uscita.

Il servizio è accessibile tramite web (webmail via https) e tramite i protocolli SMTP, per l’invio, POP3 e IMAP, per l’accesso alla casella.

L’accesso alla casella di posta Legalmail e lo scambio di messaggi avviene tramite protocollo sicuro SSL (il livello utilizzato è SSL2, ad eccezione per webmail con accesso via smartcard che utilizza SSL3) sia con client sia via Webmail. Se l’utente utilizza la posta certificata Legalmail via browser (Webmail) non è necessaria alcuna configurazione. Se invece l’utente utilizza la posta certificata Legalmail via client, l’utente deve attivare sul proprio client una connessione protetta SSL per il server di posta in arrivo (come indicato nel paragrafo 5.3). L’utente inoltre deve attivare sul proprio client la comunicazione SSL anche per l’invio di messaggi (server SMTP).

Si ricorda che è possibile inviare e ricevere messaggi con dimensione fino a 20 MB; prima di spedire un messaggio è bene verificare di avere **spazio** sufficiente per ricevere tutte le ricevute di consegna. Se il messaggio viene inviato (in “TO”) a molti destinatari di posta certificata e la dimensione del messaggio è significativa si deve considerare che ogni ricevuta di consegna ha in allegato tutto il messaggio inviato. Per acquisire correttamente tutte le ricevute di consegna si deve avere spazio sufficiente.

Inoltre la codifica “mime” degli allegati ai messaggi fa aumentare la dimensione del messaggio inviato. Questo significa che un messaggio con un allegato di 100KB potrebbe diventare durante la spedizione di 140 KB: di questo va tenuto conto nella valutazione dello spazio a disposizione nella casella quando si fanno molteplici invii in “TO” (per la ricevuta di consegna).

E’ comunque possibile acquisire ulteriore spazio disco aggiuntivo nel caso l’utente lo ritenga necessario.

5.2 Accesso via Webmail

A Webmail si accede da www.legalmail.it tramite user e password o tramite smartcard con apposito certificato di autenticazione.

Per accedere al servizio è necessario avere un Personal Computer dotato di un browser Internet Explorer 5.50 o superiore oppure prodotti equivalenti.

L'utilizzo della "modalità avanzata" con la possibilità "firmare" e "crittografare" il messaggio comporta lo scaricamento e l'installazione automatica sulla stazione di lavoro di alcuni prodotti software per la firma e la crittografia (java plug-in, librerie di firma digitale, applet). Se la stazione di lavoro fosse priva di tutti questi prodotti, sarà necessario acquisire diversi MB di software; pertanto si consiglia di fare la prima attivazione della modalità avanzata solo avendo a disposizione una connessione veloce ad Internet.

Per firmare e crittografare i messaggi di posta elettronica è necessario avere una smartcard InfoCamere con il certificato di autenticazione contenente l'indirizzo della casella di posta utilizzata.

Per motivi di sicurezza si consiglia di cambiare subito la password fornita inizialmente. Il cambio password è accessibile nella sezione "Opzioni" di webmail.

5.3 Accesso via client

Per accedere alla Posta Certificata InfoCamere attraverso un client di posta è necessario utilizzare Outlook 5.50 o superiore, oppure prodotti equivalenti. E' inoltre necessario configurare il client con gli opportuni parametri come sotto descritto.

I parametri per la configurazione della posta Certificata Infocamere sono:

- Tipo di server: POP3/IMAP
- Server di posta in arrivo: mbox.cert.legalmail.it
- Server di posta in uscita: sendm.cert.legalmail.it

L'utente si deve autenticare al server di posta in uscita (settare l'opportuno parametro).

Il server di posta in arrivo necessita di una connessione protetta, utilizza la porta POP3S (995) o IMAPS (993) (settare l'opportuno parametro).

Inoltre è necessario utilizzare la connessione protetta SSL anche per la posta in uscita (SMTP). Si consiglia di utilizzare per l'invio la porta 465 al posto della 25; l'Outlook lascia per default la porta 25, è tuttavia possibile configurare l'uso della 465. Si sono riscontrati infatti dei problemi in fase di invio con l'uso della porta di default se il client è protetto da alcune tipologie di antivirus.

Per firmare e crittografare i messaggi di posta elettronica è necessario avere una smartcard rilasciata da un Ente Certificatore (Es. InfoCamere) con il certificato di autenticazione contenente l'indirizzo della casella di posta utilizzata.

Le userid e password da utilizzare sono quelle fornite all'atto della sottoscrizione del contratto.

Per motivi di sicurezza si consiglia di cambiare subito la password fornita inizialmente. Il cambio password è accessibile nella sezione "Opzioni" di webmail.

5.3.1 Configurazione Outlook Express con Internet Explorer 5.5 o superiore

Descriviamo le operazioni necessarie per configurare Outlook Express

Definizione nuovo utente di posta:

1. Avviare Outlook Express da: Start – Programmi – Outlook Express;
2. Selezionare "Strumenti"(Tools) quindi "Account";
3. Dalla finestra "Account Internet" selezionare "Aggiungi" (Add) e quindi "Posta elettronica" (Mail);
4. Su "Display Name": Digitare Nome e Cognome o altro identificativo e premere "Avanti ";
5. Selezionare "Utilizza l'indirizzo già disponibile" (I already have an Email address that I'd like to use) e indicare l'indirizzo completo fornito da InfoCamere (es. mario.rossi@legalmail.it). Premere "Avanti ";
6. Nella finestra "Nomi dei server della posta" (Internet Connection Wizard) fra le tre opzioni proposte per la posta in arrivo selezionare POP3 (consigliato) o IMAP, impostare come server di posta in arrivo (Incoming mail server): "mbox.cert.legalmail.it" e impostare come server di posta in uscita (Outgoing mail SMTP server): "sendm.cert.legalmail.it" quindi premere "Avanti";
7. Nella finestra successiva, come Nome Account (Account Name) digitare lo userid fornito da InfoCamere. Si consiglia di non inserire la password. Premere "Avanti";
8. Premere "Fine", ricomparirà la finestra "Account Internet" (Internet Accounts);
9. Selezionare l'utente appena definito e premere "Proprietà" (Properties);
10. Selezionare la scheda "Impostazioni Avanzate" (Advanced), alla voce "Posta in arrivo (POP3 o IMAP)" (Incoming Mail (POP3 o IMAP)) comparirà il numero 110 o 143, selezionare la casella sottostante "il server necessita di una connessione protetta (SSL)" (This server requires a secure connection (SSL)), il numero verrà modificato in 995 o 993. Selezionare quindi "Applica" (Apply);
11. Selezionare la scheda "Impostazioni Avanzate" (Advanced), alla voce "Posta in uscita (SMTP)" (Outgoing Mail (SMTP)), selezionare la casella sottostante "il server necessita di una connessione protetta (SSL)" (This server requires a secure connection (SSL)), il numero indicato è 25; indicare 465 come porta. Selezionare quindi "Applica" (Apply);
12. Selezionare la scheda "Server", settare l'ultima casella "Autenticazione del server necessaria" (Outgoing server user name) e premere "OK";
13. Selezionare "Chiudi" (Close).

A questo punto l'utente di posta è pronto ad operare, quindi a scaricare ed inviare posta.

Per ulteriori informazioni

info.legalmail@infocamere.it

www.legalmail.it

InfoCamere

Direzione Generale

Via G. B. Morgagni, 30H

00161 Roma

Sede Operativa e Amministrativa

Corso Stati Uniti, 14

35127 Padova