

“InfoCert”

LEGALMAIL Posta Certificata
Manuale utente

The logo for Legalmail, with the word "Legalmail" in a blue, sans-serif font. The letter "l" is stylized with a circular dot.

Indice

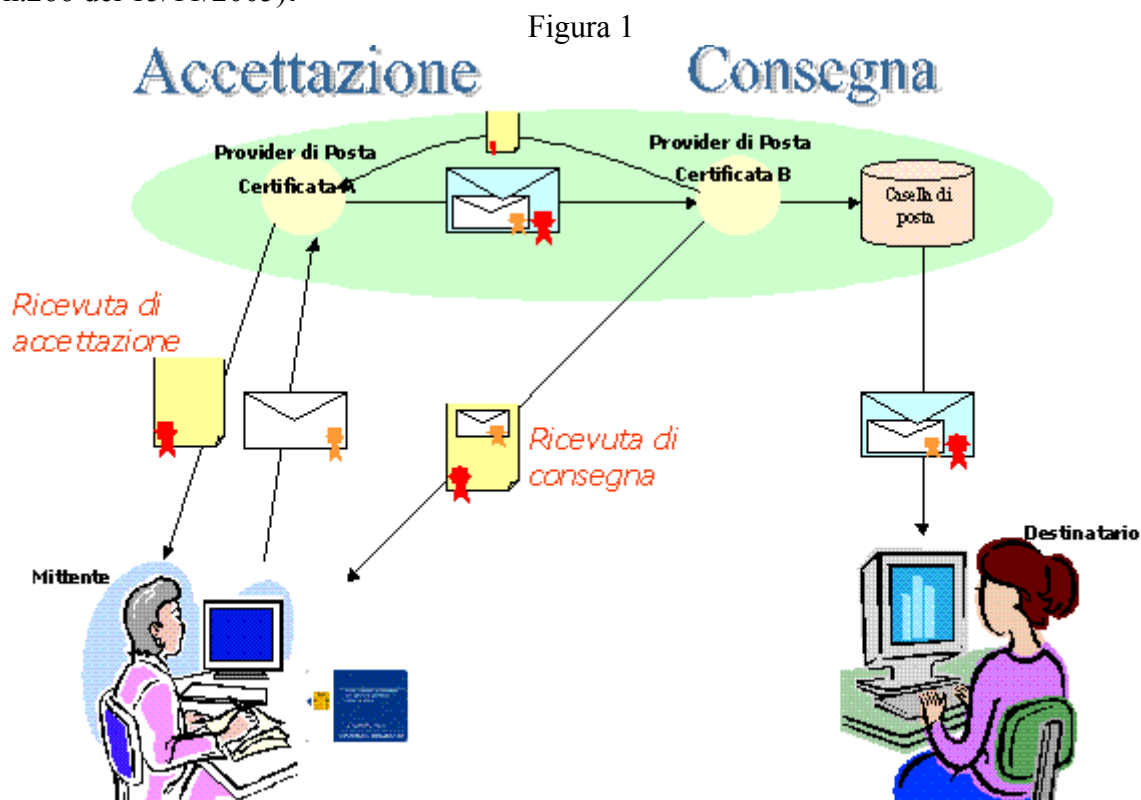
1.Introduzione al servizio di posta elettronica certificata.....	4
2.Legalmail: il servizio di posta elettronica certificata InfoCert.....	6
2.1Funzionalità standard.....	6
2.2Norme di utilizzo per l'utenza	7
3.Certificati utilizzati dai gestori di posta certificata.....	9
3.1Firma gestita.....	9
3.2Accettazione certificati.....	9
3.3Certificati scaduti.....	10
4.I messaggi di posta certificata	11
4.1Elaborazione dei messaggi.....	11
4.1.1La ricevuta di accettazione e la busta di trasporto, per l'invio.....	11
4.1.2Gli avvisi di non accettazione per eccezioni formali e per virus informatico.....	11
4.1.3Le ricevute di preso in carico.....	11
4.1.4La ricevuta completa di avvenuta consegna.....	11
4.1.5La ricevuta breve di avvenuta consegna.....	12
4.1.6La ricevuta sintetica di avvenuta consegna.....	12
4.1.7La busta di anomalia per i messaggi provenienti da caselle di posta non certificata	12
4.1.8L'avviso di rilevazione virus informatico.....	12
4.1.9Gli avvisi di mancata consegna, nei casi previsti.....	12
4.1.10La generazione di tutti i file xml previsti dalla normativa.....	13
4.1.11L'inserimento del riferimento temporale in tutti i messaggi/log previsti.....	13
5.Il flusso dei messaggi tra domini di posta certificata.....	14
5.1Qui di seguito sono descritti i flussi con alcuni dettagli aggiuntivi.....	14
5.2Messaggio da posta normale a posta certificata	16
5.3Messaggio da posta certificata a posta normale.....	17
5.4Note e particolarità dei messaggi di posta certificata.....	17
6.Accesso a LEGALMAIL.....	19
6.1Firma dei messaggi da parte del mittente (opzionale).....	19
6.2Firma degli allegati al messaggio.....	19
6.3Dimensioni casella e messaggi.....	20
6.4Raccomandazioni generali per l'utenza.....	20
7.Accesso tramite browser.....	22
7.1.1Requisiti tecnici	22
8.Accesso tramite client di posta elettronica	23
8.1Requisiti tecnici	23
8.2Esempio di configurazione Outlook Express con Internet Explorer 5.5 o superiore	23
9.Accesso al sistema WEBMAIL attraverso il sito LEGALMAIL.....	25
9.1Accesso a Webmail.....	25
9.2La maschera Principale: La mia posta.....	26
9.3La console	27
9.4Opzioni.....	27
9.4.1Opzioni: Generale.....	28
9.4.2Opzioni: Scrivi.....	28
9.4.3Opzioni: Password.....	29
9.4.4Opzioni: Filtri.....	29

Inoltro automatico.....	31
9.4.5Opzioni: SMS.....	32
9.4.6Opzioni: Contatti.....	33
9.4.7Opzioni: Storico.....	34
9.4.8Opzioni: Antispam.....	35
9.5Guida:.....	36
10.Barra degli strumenti.....	37
10.1descrizione delle funzioni.....	37
11.Lista dei messaggi e anteprima.....	38
11.1Tipologie dei messaggi.....	39
12.Gestione cartelle.....	41
13.La finestra “Visualizzazione messaggio”.....	42
13.1Ricezione di messaggi crittografati.....	44
14.Nuovo Messaggio.....	45
14.1Descrizione dei campi:.....	46
15.Rubrica.....	48
15.1Inserire un gruppo in rubrica:.....	49
15.2Inserire un contatto in rubrica:.....	50
16.“Rispondi”, “Rispondi a tutti” e “Inoltra”.....	52
17.Ricerca.....	53
18.Ricerca Storico.....	54
19.Segnalazioni di esaurimento dello spazio a disposizione.....	55
20.Esempi di messaggi di posta certificata.....	56
20.1.1Ricevuta di Accettazione.....	56
20.1.2Messaggio di Posta Certificata.....	59
20.1.3Ricevuta di Consegna.....	61
20.1.4Messaggio da posta ordinaria:.....	62
21.Malfunzioni connesse alla firma elettronica.....	63
22.Termini e definizioni.....	64
22.1Riferimenti normativi e tecnici.....	64
22.2Definizioni.....	64
22.3Acronimi e abbreviazioni.....	66

1. Introduzione al servizio di posta elettronica certificata

La seguente rappresentazione grafica illustra schematicamente il servizio di posta elettronica certificata. Questa breve descrizione non vuole essere una descrizione tecnica esaustiva del servizio, ma vuole introdurre l'utente in modo semplice ed intuitivo alle specificità del servizio di posta elettronica certificata.

Di seguito, in questo stesso documento, sono approfonditi tutti i punti del servizio come richiesto dalla normativa sancita dal Decreto Ministeriale del 2 novembre 2005 recante “Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata” (GU n.266 del 15/11/2005).



L'utente, 'mittente' dopo aver superato la fase di identificazione ed autenticazione al sistema che ne convalida le credenziali, è in grado di inoltrare un messaggio.

Nel caso illustrato il mittente utilizza una funzionalità opzionale e comune a qualsiasi sistema di posta: inoltra un messaggio 'firmato', utilizzando la chiave privata memorizzata sul proprio dispositivo di firma. La firma del messaggio e/o dei suoi allegati non è comunque obbligatoria: il sistema di posta elettronica certificata accetta messaggi non firmati, firmati, crittografati e non.

Il messaggio (la busta bianca in figura 1) raggiunge il sistema del proprio provider dove viene analizzato per verificare la sua conformità alle regole di posta elettronica certificata e, in caso positivo, è imbustato in un altro messaggio, a sua volta firmato dal gestore di posta, ed inoltrato verso la sua destinazione.

Il mittente riceve in questo caso la '*ricevuta di accettazione*' firmata dal proprio gestore ed ha così la prova che il suo messaggio è stato correttamente acquisito dal sistema.

Nel caso in cui il gestore non possa accettare il messaggio, il mittente riceverà un avviso ('*avviso di non accettazione*') con il motivo della mancata accettazione da parte del sistema.

La figura illustra il caso in cui mittente e destinatario appartengono a domini gestiti da provider diversi, pertanto il messaggio deve transitare dal dominio A al dominio B.

Il gestore del destinatario (dominio B) notifica con la '*ricevuta di presa in carico*' al gestore del mittente (dominio A) che ha preso in carico con successo il messaggio.

Il transito del messaggio è così tracciato, in modo da poter rispondere comunque al mittente riguardo all'iter percorso dal suo messaggio.

Il provider di posta del dominio B deposita il messaggio nella casella del destinatario e notifica il successo dell'operazione al mittente tramite la *'ricevuta di consegna'* che contiene anche in allegato il messaggio originale, a meno che il mittente non richieda diversamente.

Il messaggio è ora disponibile al destinatario che lo può leggere a sua discrezione.

In totale il mittente riceverà almeno 2 ricevute per ogni invio: una *'ricevuta di accettazione'* e una *'ricevuta di consegna'*.

Se il mittente invia un messaggio a più destinatari con un unico invio riceverà una *ricevuta di consegna* per ogni destinatario di pec, per cui normalmente le ricevute saranno in totale in numero pari al numero dei destinatari +1 (*ricevuta di accettazione*)

Nel caso in cui si verificano eventi particolari (rilevazione virus, destinatari errati, ...) si possono ricevere altre segnalazioni; nel caso di destinatari di posta non certificata potranno mancare alcune ricevute.

L'emissione della ricevuta di consegna non è legata al fatto che il destinatario apra il messaggio o meno ed è rilasciata comunque quando il messaggio è depositato in casella; questa è una delle peculiarità del sistema di posta elettronica certificata.

Le notifiche dei sistemi di posta ordinari sono di fatto legate all'apertura del messaggio e alla volontà del mittente di far pervenire la notifica di avvenuta ricezione al mittente: una notifica di questo tipo non ha però il valore legale di opponibilità a terzi delle ricevute rilasciate e firmate da gestori accreditati.

2. Legalmail: il servizio di posta elettronica certificata InfoCert

Il servizio di posta elettronica certificata che garantisce un elevato grado di affidabilità e sicurezza, è erogato da InfoCert sotto il nome Legalmail. Esso consente al Cliente di disporre di caselle di posta elettronica certificata, che permettono di comunicare con altre caselle di stessa tipologia sulla rete mondiale Internet.

Il servizio permette inoltre di inviare, ricevere e consultare i messaggi di posta elettronica ordinaria.

L'utilizzo di caselle di Posta Elettronica Certificata garantisce al cliente l'accesso sicuro alla propria casella di posta elettronica, sia attraverso un client di posta (Thunderbird, Outlook Express, ...), sia direttamente da Internet utilizzando i più comuni browser (il servizio viene definito Webmail).

Il servizio include l'invio nella casella del cliente delle diverse tipologie di ricevute descritte nel capitolo precedente.

Le caselle di posta elettronica certificata, diversamente dalle usuali caselle di posta elettronica, consentono l'invio di posta elettronica con valore legale in conformità di quanto previsto dal CAD -Codice Amministrazione Digitale - [2]

Nei casi consentiti dalla legge, la posta certificata può essere utilizzata in *sostituzione *della posta cartacea (articolo 48 comma 2 Codice dell' Amministrazione Digitale[2]).

I messaggi ricevuti nella casella di posta certificata del destinatario si intendono *consegnati* al titolare della casella (articolo 3 comma 1 DPR 68/2005).

Si ricorda che, in base al DPR 68/2005 [8], la validità legale del messaggio di posta certificata è subordinata alla dichiarazione di disponibilità all'utilizzo della posta elettronica certificata.

2.1 Funzionalità standard

Le funzionalità più rilevanti, attivate dal gestore del servizio in conformità alla normativa ufficiale sono:

- invio al mittente di una ricevuta di accettazione per ogni messaggio in uscita che sia conforme ai requisiti normativi.
- inserimento dei messaggi in uscita dalla casella del mittente in una busta cosiddetta “di trasporto” firmata dal Gestore. La busta di trasporto è consegnato senza modifiche nella casella di posta di destinazione.
- emissione di una ricevuta di consegna per ogni destinatario al quale il messaggio risulta consegnato, se il messaggio è inviato ad una casella di posta elettronica certificata con valore legale (previsto dal CNIPA)
- inserimento dei messaggi in ingresso, non provenienti da caselle di posta elettronica certificata, in una busta “di anomalia”
- la firma elettronica del Gestore del servizio di posta elettronica certificata sulle ricevute e sulla busta di trasporto che contengono sempre informazioni relative al messaggio (time (ora), from (da), to (a), ecc.) sia in formato testo leggibile sia in formato XML

- allineamento al tempo ufficiale coordinato (UTC) dell'ora delle ricevute e del messaggio di trasporto, a meno di un secondo
- invio, in allegato alla ricevuta di consegna al mittente, di tutto il messaggio originario (come prova di quanto ha spedito ed è stato consegnato) per ogni destinatario in “TO (A)”, a meno di richiesta diversa da parte del mittente
- conservazione di un log degli eventi principali; il sistema mantiene traccia delle operazioni svolte, memorizzando su un registro i dati significativi dell'operazione: il codice identificativo univoco del messaggio (Message-ID), la data e l'ora dell'evento, il mittente del messaggio originale, l'oggetto del messaggio, etc.; il sistema non serba alcuna informazione che permetta di risalire al contenuto del messaggio, a meno di richiesta diversa da parte del cliente o di disposizioni normative specifiche.
- ricevuta di presa in carico tra diversi provider di posta del circuito (non visibile agli utenti, ma fondamentale per tenere traccia dell'iter completo percorso dal messaggio)

Le precedenti funzionalità saranno soggette a tutte le variazioni necessarie in caso di evoluzione della normativa e delle disposizioni da parte del CNIPA.

2.2 Norme di utilizzo per l'utenza

L'utente di posta certificata dovrà ottemperare alle norme seguenti per inviare un messaggio di posta elettronica certificata che sia accettato dal sistema:.

- **divieto di utilizzare dei destinatari nascosti (BCC o CCN)**
- **obbligo di indicare almeno un destinatario in "TO (A)".**
- **indirizzare il messaggio al massimo a 250 destinatari diretti (To (a))**
- **indirizzare il messaggio al massimo a 500 destinatari totali (To (a) e Cc)**

In caso contrario il sistema rifiuterà il messaggio segnalando l'evento con il messaggio di “Avviso di non accettazione”.

InfoCert mette in grado l'utente di usufruire delle funzionalità elencate attraverso il servizio Legalmail che pertanto comprende:

- **rilascio della casella di posta elettronica certificata e relativa userid per l'accesso**
- **assegnazione di una password e riassegnazione e cambio su richiesta dell'utente**
- **accesso alla casella da client di posta**
- **spedizione di messaggi con client di posta**
- **accesso alla casella e spedizione di messaggi con webmail**
- **possibilità di firmare e crittografare i messaggi attraverso webmail (in ambiente windows e utilizzando smart card e certificati emessi dal Certificatore InfoCert**

[www.card.InfoCert.it) o attraverso il client di posta (utilizzando smart card e certificati emessi sia da InfoCert che da altri Enti Certificatori)

- possibilità di salvare da webmail i messaggi su disco
- utilizzo del sito legalmail (www.legalmail.it) con informazioni di supporto
- call center per il supporto informativo
- presenza di un antivirus aggiornato che controlla i documenti e i messaggi in entrata e in uscita.

Ove non espressamente indicato in modo diverso si applicano i seguenti limiti:

- la dimensione della casella di posta elettronica certificata è non inferiore a 100 MB.
- la dimensione massima del messaggio prevista è 30 MB.

Questa dimensione ammissibile diminuisce al crescere dei destinatari, come indicato nel Paragrafo [Dimensioni casella e messaggi](#)

Il servizio di posta elettronica certificata Legalmail è conforme alle regole tecniche e organizzative indicate dalla normativa in riferimento, ed esattamente:

- DPR 11 febbraio 2005, n. 68, “Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata”;
- DM 2/11/2005 recante “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata”
- Allegato tecnico al DM indicato al punto precedente “Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata”

3. Certificati utilizzati dai gestori di posta certificata

I messaggi e le ricevute di posta elettronica certificata / posta elettronica a valore legale sono email firmate dai gestori del servizio (gestore del mittente / gestori dei destinatari) mediante appositi **certificati** (detti anche **id digitali**).

Quando si riceve un messaggio di posta firmato lo strumento di consultazione della posta (XLegalMail oppure un client tipo Outlook, Mozilla, ...) può:

- a) *non gestire la firma*, se si tratta di uno strumento vecchio; lo strumento probabilmente mostra la firma come se fosse un ulteriore file allegato al messaggio
- b) *gestire la firma*, se si tratta di uno strumento abbastanza recente

3.1 Firma gestita

Lo strumento, quando riceve un messaggio firmato, effettua delle verifiche. Se qualche verifica non va a buon fine all'utente viene segnalato un problema. La segnalazione varia da strumento a strumento, alcuni si limitano a piccole immagini con un elemento rosso, con una x, ... altri strumenti, come Outlook, presentano una schermata completamente nera (che mette in allarme molti utenti).

3.2 Accettazione certificati

Quando uno strumento di posta riceve un messaggio firmato con un certificato sconosciuto può segnalare il problema (in modo più o meno allarmante).

Il certificato utilizzato per la firma dei messaggi di posta certificata è rilasciato dal CNIPA e firmato a sua volta da un certificato presente nei comuni client di posta. Questo permette al client di posta di riconoscere i messaggi senza segnalare particolari anomalie.

Può comunque capitare, in base al client di posta, che vengano segnalate anomalie, in particolare:

- la prima volta che usa la posta certificata / a valore legale
- ogni volta che un gestore cambia certificati
- ogni volta che si comunica con nuove caselle, di un gestore nuovo

I gestori di posta devono cambiare periodicamente i certificati perché questi ultimi valgono per un periodo limitato di tempo (ogni certificato ha una scadenza).

Per non vedere più l'allarme (schermata nera, ...) è sufficiente accettare i nuovi certificati come validi.

Per accettare si può (a seconda degli strumenti in uso):

- 1) accettare il certificato al momento della ricezione del messaggio
- 2) installare il certificato dell'ente che emette questi certificati: tutti i certificati dei gestori sono emessi dal CNIPA; è possibile quindi installare il certificato della CA emittente i certificati (è possibile scaricare il certificato al link "<http://www.legalmail.it/webreg/CnipaCA2.crt>").

L'installazione del certificato dipende dal client; è sufficiente selezionare il link indicato con il browser e procedere alla installazione del certificato con l'apposita procedura (Outlook), oppure scaricare su disco locale il certificato e installarlo nel client tramite le opzioni di quest'ultimo.

3.3 Certificati scaduti

I certificati usati dai gestori per la firma hanno una data di scadenza. Se si consulta un messaggio o una ricevuta dopo la data di scadenza del certificato con cui è stato firmato, lo strumento di posta segnalerà che il certificato è scaduto (in modo più o meno allarmante).

Per verificare comunque la validità della trasmissione è sufficiente confrontare la data di trasmissione (presente nel messaggio / busta) con la data di scadenza del certificato (bisogna visualizzare i dati del certificato: i più comuni strumenti di gestione della posta lo consentono): la data di scadenza del certificato deve essere successiva a quella di trasmissione.

Per prolungare la validità, a fini legali, di un file (o messaggio) firmato si può apporre una marca temporale rivolgendosi ad una Certification Authority accreditata al CNIPA (ad esempio InfoCert: www.card.infocert.it).

caselle di posta elettronica certificata distribuite dal CNIPA stesso o da altri gestori di posta certificata accreditati.

4. I messaggi di posta certificata

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 per la posta certificata 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".

4.1 Elaborazione dei messaggi

Il sistema garantisce il rispetto di tutte le regole previste per la posta elettronica certificata dai documenti in riferimento [8] e [5], in particolare delle norme riguardanti l'elaborazione e lo scambio di messaggi tra caselle di posta elettronica certificata elencate di seguito:

4.1.1 La ricevuta di accettazione e la busta di trasporto, per l'invio

Il sistema di posta elettronica certificata notifica all'utente attraverso la ricevuta di accettazione il successo dell'invio di un messaggio, dato dal superamento di tutti i controlli formali e di contenuto (ad esempio viene controllata la presenza nel messaggio di virus informatici) e lo rende conforme al sistema 'imbustandolo' nella busta di trasporto.

Il tempo previsto per il rilascio della ricevuta di accettazione, così come previsto all'articolo 12 comma 6 del DM [5], è concordato tra Gestore e Titolare, secondo le specifiche esigenze; in mancanza di accordo specifico tra le parti le ricevute di accettazione verranno rilasciate entro un tempo di 30 minuti nel 99% dei casi su base quadrimestrale.

4.1.2 Gli avvisi di non accettazione per eccezioni formali e per virus informatico

Il sistema di posta elettronica certificata notifica all'utente la non accettazione del messaggio e la motivazione per cui è stato respinto.

Un motivo di non accettazione di un messaggio per errore formale è, per esempio, la violazione della regola di posta elettronica certificata che non permette l'utilizzo nel campo "From (Da)" di un indirizzo di email diverso da quello proprio della casella dell'utente mittente cioè quella che corrisponde alle credenziali utilizzate per accedere al servizio. E' inoltre necessario che vi sia congruenza tra il from (da) utilizzato a livello di protocollo SMTP ed il from (da) indicato all'interno del messaggio di posta

4.1.3 Le ricevute di preso in carico

Il sistema di posta elettronica certificata del circuito notifica all'altro la presa in carico del messaggio che transita tra domini diversi, per tracciare completamente l'iter del messaggio; queste ricevute non pervengono all'utente, ma solo ai gestori del servizio.

4.1.4 La ricevuta completa di avvenuta consegna

L'utente riceve dal sistema di posta elettronica certificata un messaggio di notifica dell'avvenuto inserimento, del messaggio inviato, nella casella di posta elettronica certificata del destinatario. Nel caso usuale il sistema invia una ricevuta completa con, in allegato, i dati di certificazione e il messaggio originale per i destinatari diretti in 'to (a)'.

4.1.5 La ricevuta breve di avvenuta consegna

A richiesta dell'utente, in sostituzione della ricevuta completa, il sistema invia una ricevuta breve con, in allegato, i dati di certificazione ed un estratto del messaggio originale.

E' indispensabile che, in questo caso, l'utente conservi il messaggio originale o gli allegati in esso contenuti se reputa che sia necessario dimostrare, oltre all'invio e alla avvenuta consegna del messaggio nella casella del destinatario, anche il contenuto del messaggio stesso.

L'estratto del messaggio non è infatti leggibile di per se, ma può essere associato tramite strumenti informatici (funzioni di hash), soltanto al messaggio che lo ha generato, rendendolo così opponibile a terzi.

Nel caso il messaggio originale non sia disponibile o sia stato alterato anche in minima parte, l'opponibilità non sarà più praticabile.

4.1.6 La ricevuta sintetica di avvenuta consegna

Per destinatari di posta elettronica certificata in copia 'Cc' la notifica avviene tramite una ricevuta sintetica con in allegato solo i dati di certificazione.

La ricevuta sintetica può essere richiesta anche per i destinatari in TO; in questo caso, tuttavia, si perde la certificazione sul contenuto dell'invio e rimane solo la certificazione sull'oggetto / data e ora / mittente / destinatario.

Il motivo di non allegare ad ogni tipo ricevuta il messaggio originale completo risiede nel obiettivo di salvare spazio nella casella dell'utente, evitando di riempirla con messaggi potenzialmente molto onerosi e, nel caso di invii multipli, ridondanti.

4.1.7 La busta di anomalia per i messaggi provenienti da caselle di posta non certificata

Quando un messaggio non di posta elettronica certificata è recapitato ad una casella di posta elettronica certificata, viene inserito in una busta di anomalia per evidenziare l'evento, in modo che il destinatario possa distinguere agevolmente i messaggi certificati dagli altri. Normalmente l'anomalia è dovuta al fatto che il messaggio di posta proviene da un mittente estraneo al circuito di posta elettronica certificata

4.1.8 L'avviso di rilevazione virus informatico

Il servizio di posta elettronica certificata si pone come obiettivo anche quello di garantire, in modo più efficace rispetto ai sistemi di posta ordinari, la sicurezza dei propri utenti anche dalla ricezione e propagazione di virus informatici.

I messaggi di posta elettronica certificata con virus informatici non sono infatti inoltrati, ma sono bloccati e il gestore del destinatario genera un avviso di rilevazione virus da restituire al gestore mittente indicando come indirizzo quello specificato per le ricevute nell'Indice dei gestori di posta elettronica certificata, con l'indicazione dell'errore riscontrato. Questo messaggio non è inoltrato all'utente, ma è utilizzato dal gestore del mittente per notificare al proprio utente l'impossibilità di consegnare il messaggio.

4.1.9 Gli avvisi di mancata consegna, nei casi previsti

Il mittente riceve sempre notifica dell'esito della spedizione di un messaggio. Nel caso il messaggio non possa essere recapitato, il mittente riceverà un avviso di mancata consegna con il motivo per cui il sistema non ha potuto depositare il messaggio nella casella di destinazione. Alcuni casi di errore, come un indirizzo errato e l'avviso che la casella di destinazione non ha lo spazio necessario per MU/PEC – Legalmail Posta Certificata Manuale utente - Ver. 1 del 15/01/2008

depositare il messaggio, forniscono all'utente delle indicazioni utili sulle azioni da intraprendere per poter inviare correttamente il messaggio.

4.1.10 La generazione di tutti i file xml previsti dalla normativa

Questi file contengono dati che descrivono il messaggio (data e ora di invio, mittente, destinatario, oggetto, identificativo del messaggio etc.) e sono utilizzati dai sistemi di posta elettronica certificata per elaborazioni automatiche.

4.1.11 L'inserimento del riferimento temporale in tutti i messaggi/log previsti

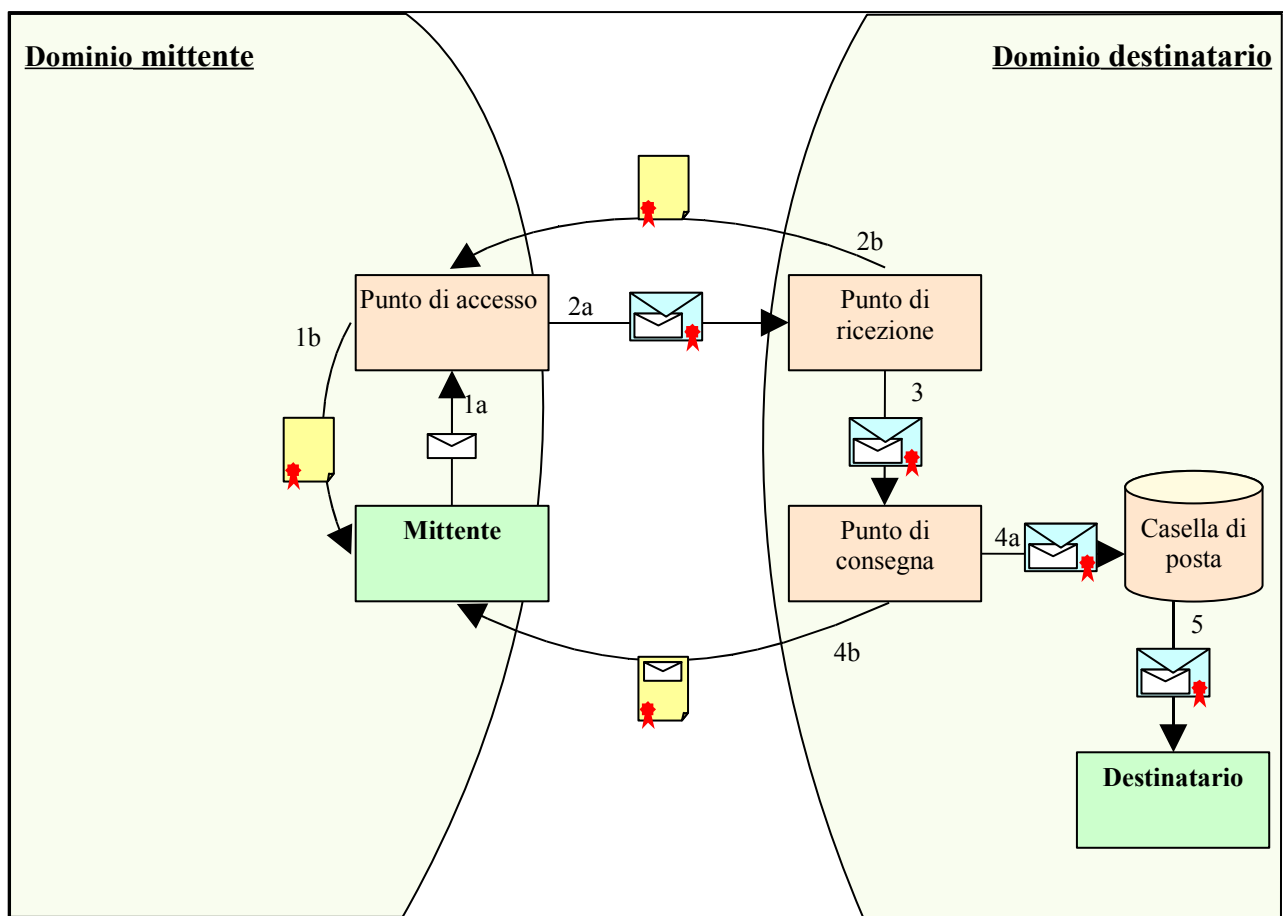
il riferimento temporale ha un errore inferiore al secondo rispetto al Tempo Universale Coordinato (UTC).

La conservazione per 30 mesi dei log con gli eventi principali riguardanti i messaggi in transito. La normativa prevede che nel registro di log certificato siano registrate le seguenti informazioni:

- il codice identificativo univoco assegnato al messaggio originale
- la data e l'ora dell'evento
- il mittente del messaggio originale
- i destinatari del messaggio originale
- l'oggetto del messaggio originale
- il tipo di evento (accettazione, ricezione, consegna, ricevute, errore, ecc.)
- il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.)
- il gestore mittente

La possibilità di reperire queste informazioni presso tutti i gestori di posta elettronica certificata garantisce all'utente la possibilità di avere, entro un periodo di 30 mesi dall'invio, gli elementi, opponibili a terzi, relativi all'invio effettuato, all'iter del messaggio e all'esito dell'invio stesso.

5. Il flusso dei messaggi tra domini 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 (1b)**
- 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 (4b)**
- 5) Il destinatario accede alla propria casella per leggere i messaggi ricevuti

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

5.1 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 fa qualche controllo sul messaggio; se non ci sono 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.

Si ricorda che 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 (**2b**) 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; in altri casi no.

4a – Il provider del destinatario (punto di consegna) deposita il messaggio nella casella del destinatario. Il messaggio si compone del 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.

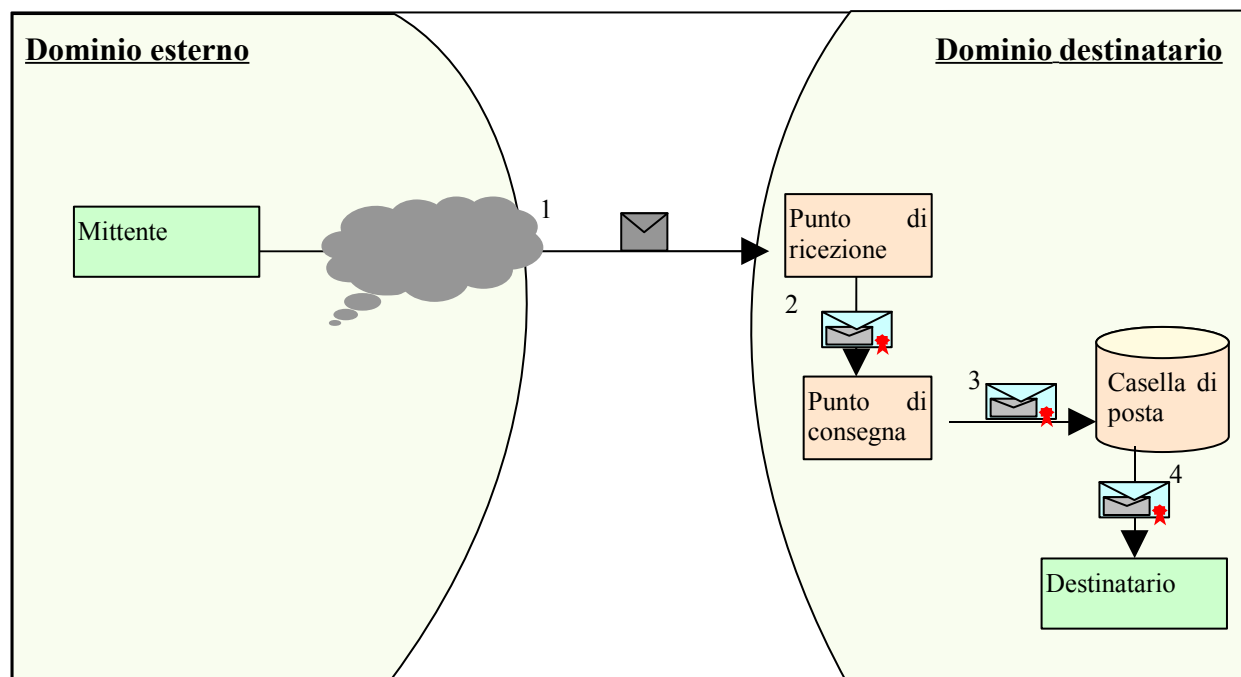
Attenzione: prima di spedire un messaggio è bene verificare di avere **spazio** sufficiente per ricevere tutte le ricevute di consegna. Se il messaggio viene inviato (in “TO”) a molti destinatari di posta certificata e la dimensione del messaggio è significativa si deve considerare che ogni ricevuta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

5.2 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)



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)

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)

Il messaggio di anomalia, a cui è allegato il messaggio ricevuto, viene depositato nella casella del destinatario (3).

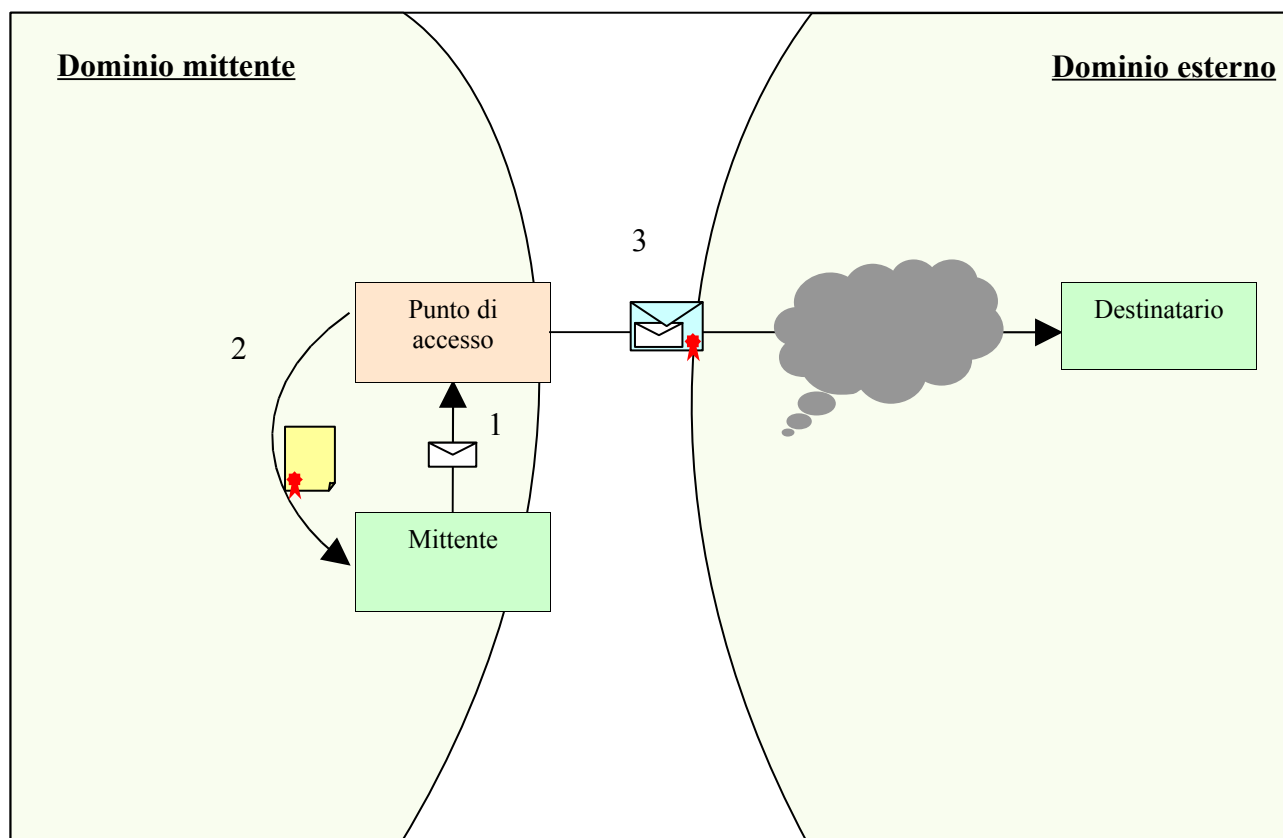
Il destinatario accede alla casella di posta e legge il messaggio di anomalia che contiene il messaggio originale (4).

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.

5.3 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



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

Il provider fa qualche controllo sul messaggio; se non ci sono 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)

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).

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.

5.4 Note e particolarità dei messaggi di posta certificata

Si ricorda che un messaggio si intende di posta certificata solo se mittente e destinatario hanno entrambi una casella di posta certificata e che, 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 45 comma 2 del Codice dell'Amministrazione Digitale (Il documento informaticosi intende consegnato al destinatario se reso disponibile nella casella di posta elettronica del destinatario).

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 XLegalMail. Inoltre è possibile inviare messaggi allegando documenti firmati con la firma di sottoscrizione a norme AIPA.

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/BusinessKey rilasciata da InfoCert (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. [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 risulterà corretto: verrà inserito l'indirizzo del provider del mittente e i messaggi spediti non arriveranno mai alla giusta destinazione.

6. 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).

Per accedere al servizio Legalmail occorrono:

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

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).

6.1 Firma dei messaggi da parte del mittente (opzionale)

Per firmare digitalmente i messaggi di posta occorre:

- certificato di autenticazione, rilasciato dall'Ente Certificatore InfoCert nel caso l'utente utilizzi webmail via browser (in ambiente windows):
- certificato di autenticazione, rilasciato da un Ente Certificatore (per esempio InfoCert) 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 come indicato nel sito <http://www.firma.infocert.it>

6.2 Firma degli allegati al messaggio

Per firmare digitalmente i documenti informatici occorre:

- certificato di sottoscrizione a norma del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) rilasciato dall'Ente Certificatore (es. InfoCert) con il relativo dispositivo di firma
- **DiKe**, il software InfoCert per firmare digitalmente i documenti (download gratuito dal sito <http://www.firma.infocert.it/installazione/software.php>) nel caso si utilizzi un certificato InfoCert oppure altri strumenti di firma nel caso si utilizzi altro certificato.

6.3 Dimensioni casella e messaggi

È possibile richiedere espansioni della dimensione standard delle caselle (100 MB) con incrementi di 100 MB (cumulabili).

Si ricorda che la massima dimensione complessiva di un messaggio è pari a 30 MB.

Se si inviano messaggi, di grandi dimensioni, a più destinatari diretti (indicati come “To (a)”), tutti appartenenti al circuito della posta elettronica certificata, con un unico invio, è necessario assicurarsi che il prodotto del numero di tali destinatari per la dimensione del messaggio non superi i 30 MB.

Prima di spedire un messaggio di dimensioni significative è sempre bene verificare di avere spazio sufficiente per ricevere tutte le ricevute di consegna. Se il messaggio viene inviato (in “TO (A)”) a molti destinatari di posta elettronica certificata e la dimensione del messaggio è significativa si deve considerare che ogni ricevuta di consegna ha in allegato tutto il messaggio inviato, a meno di disposizioni contrarie da parte del mittente.

Per acquisire correttamente tutte le ricevute di consegna si deve avere spazio sufficiente.

Per questo motivo sono stati posti dei limiti sul numero dei destinatari per un singolo invio:

- il numero massimo di destinatari diretti (To: (A:)) è 250
- il numero massimo di destinatari totali (To: (A:) e CC:) è 500.

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 (il rapporto non è costante, si tratta di un puro esempio): di questo va tenuto conto nella valutazione dello spazio a disposizione nella casella quando si fanno molteplici invii in “TO (A)” (per la ricevuta di consegna).

Si ricorda che è possibile inviare e ricevere messaggi con dimensione fino a 10 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, a meno di disposizioni diverse del mittente. 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.

6.4 Raccomandazioni generali per l'utenza

Si ricorda che lo strumento scelto dal Cliente determina la modalità di utilizzo con esclusione delle particolarità legate al servizio di posta elettronica certificata.

Per un corretto utilizzo delle caselle di posta si suggerisce al Titolare di consultare frequentemente la casella; infatti ogni messaggio ricevuto nella casella di posta elettronica certificata si intende pervenuto al Titolare della casella stessa (DPR 68/2005 [8]).

E' bene cancellare dal server di posta i messaggi con una frequenza sufficiente per evitare che venga occupato tutto lo spazio assegnato alla casella stessa (di norma 300 MB complessivi, se non concordato direttamente) e quindi i messaggi successivi vengano rifiutati. Il servizio Legalmail tiene traccia dei soli log degli eventi principali, ma non comprende (per le caselle standard) il sistema di conservazione a norma dei documenti scambiati via posta elettronica né delle relative ricevute.

Ai fini di garantire il più alto livello di sicurezza nel controllo degli accessi, come già scritto in precedenza, si invita l'utente a cambiare al più presto la password di accesso ricevuta da InfoCert.

E' opportuno dotare le stazioni di lavoro di un antivirus costantemente aggiornato per garantire maggiore sicurezza per quanto viene spedito e ricevuto. Infatti, se pure la casella Legalmail è dotata di antivirus in grado di proteggere l'utente dai principali pericoli di infezione, non è possibile controllare automaticamente tutti i contenuti potenzialmente dannosi; in particolare si fa presente che i messaggi o file crittografati non possono essere sottoposti a controlli efficaci.

Verificare l'identità del mittente e dei destinatari con i mezzi più idonei è una prassi consigliabile. A puro titolo di esempio si cita la possibilità di utilizzare la firma di sottoscrizione apposta su un allegato al messaggio per identificare il mittente. In nessun caso il nome della casella può costituire un indizio valido per identificare con sicurezza il titolare

Portare a conoscenza dei propri corrispondenti che si è in possesso di una casella di posta elettronica certificata, costituisce una garanzia anche per i destinatari.

Perché il messaggio certificato abbia valore legale è necessaria la dichiarazione prevista dall'art 4 del DPR 68/2005

7. Accesso tramite browser

Per accedere alla posta elettronica certificata InfoCert attraverso un browser, si accede da www.legalmail.it a Webmail, tramite user-id e password o tramite smartcard con apposito certificato di autenticazione abilitato al servizio.

Per motivi di sicurezza è fortemente raccomandato che il cliente cambi subito la password fornita inizialmente.

Il cambio password è accessibile nella sezione “Opzioni” di Webmail.

Lo strumento permette di consultare la posta in arrivo, spedire messaggi di posta elettronica e organizzare la posta in arrivo.

Lo strumento consente inoltre l'utilizzo, limitatamente all'ambiente windows, delle funzioni di firma e crittografia dei messaggi con certificati InfoCert.

Per accedere al servizio è necessario avere un Personal Computer dotato di un browser Internet Explorer 5.5 (con livello di codifica 128 bit) o superiore, oppure prodotti equivalenti.

La sessione di lavoro con webmail ha una durata di tempo limitata; fatta eccezione per alcune funzionalità, dopo 15 minuti di mancata comunicazione con il sistema che gestisce webmail, il Titolare non sarà più in grado di continuare correttamente il lavoro intrapreso.

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 dotarsi di diversi MB di software; pertanto si consiglia di fare la prima attivazione della modalità avanzata avendo a disposizione una **connessione veloce** ad Internet.

Per poter firmare un messaggio di posta elettronica e/o un documento allegato, l'utente può avvalersi dei servizi di Firma Digitale forniti da InfoCert in qualità di Autorità di Certificazione .

Nel caso in cui l'utente scelga InfoCert per firmare e crittografare i messaggi di posta elettronica, sarà dotato di una smartcard InfoCert con il certificato di autenticazione contenente l'indirizzo della casella di posta utilizzata.

Tutti i dettagli e le modalità di utilizzo sono descritte nello strumento stesso attraverso la guida in linea reperibile al sito <http://www.firma.infocert.it>

7.1.1 Requisiti tecnici

E' necessario un browser che utilizzi HTTPS -protocollo sicuro- per avvalersi delle funzionalità complete di firma e crittografia. E' necessario come versione minima: Explorer 5.50, o prodotti equivalenti/superiori. La postazione dell'utente dovrà pertanto essere già dotata di accesso a internet che permetta il colloquio attraverso la porta standard:

→ **HTTP/S 443** per utilizzare webmail come strumento di invio e lettura dei messaggi

8. Accesso tramite client di posta elettronica

Per accedere alla posta elettronica certificata InfoCert attraverso un client di posta è necessario utilizzare Outlook Express 5.5 o superiore, oppure prodotti equivalenti. E' inoltre necessario configurare il client con gli opportuni parametri per definire, ad esempio, il tipo di server di posta a cui collegarsi ed i parametri utilizzati dal server stesso per eseguire le operazioni di autenticazione della casella utente.

Il server di posta in arrivo necessita di una connessione protetta, utilizza la porta POP3S o IMAPS e inoltre è necessario utilizzare la connessione protetta SSL anche per la posta in uscita (SMTP).

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

8.1 Requisiti tecnici

L'utente che acceda al servizio di posta elettronica certificata dovrà dotarsi di client che utilizzi POP3-S e IMAP-S, utilizzando un client di posta standard come Outlook 5.50, o prodotti equivalenti/superiori. La postazione dell'utente dovrà pertanto essere già dotata di accesso a internet che permetta il colloquio attraverso la porta standard:

- **SMTP/SSL 465** per spedire messaggi con client di posta (consigliato)
- **SMTP STARTTLS 25** per spedire messaggi 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

8.2 Esempio di 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 InfoCert (es. mario.rossi@cert.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 InfoCert. 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. 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.

9. Accesso al sistema WEBMAIL attraverso il sito LEGALMAIL

Nei prossimi paragrafi sono descritte le caratteristiche di Webmail: si consiglia di accedere a Webmail appena ricevuta la casella di posta per cambiare la password iniziale.

Per accedere a Webmail è possibile collegarsi al sito www.legalmail.it accedendo tramite user e password (LOGIN) o tramite smartcard con apposito certificato di autenticazione (LOGIN con CARD).

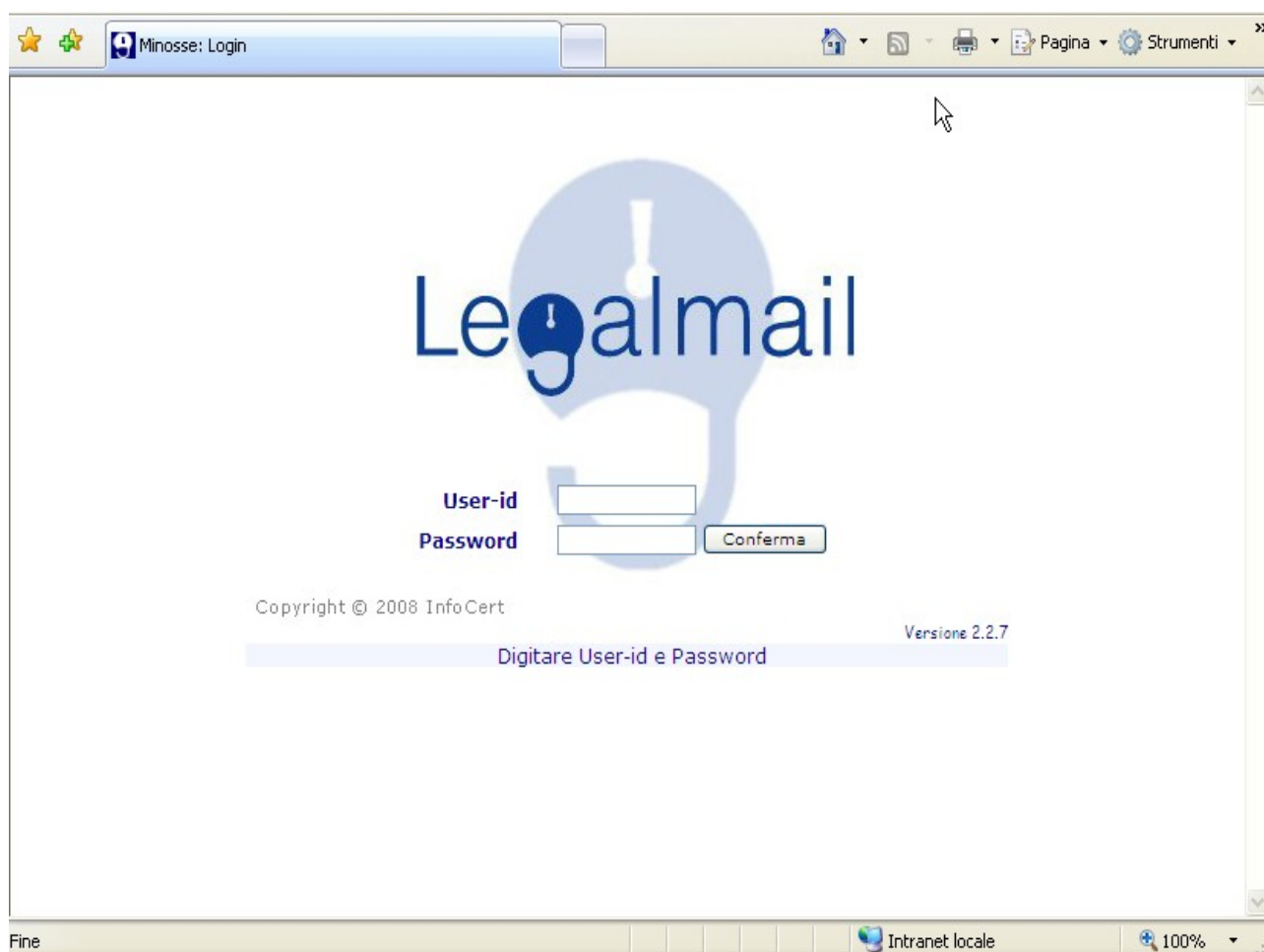
Se l'utente accede attraverso LOGIN, indicare le proprie credenziali e selezionare "Entra".

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.

9.1 Accesso a Webmail

La nuova versione di Legalmail è progettata per rendere l'esperienza con la Posta Elettronica Certificata più gradevole e in linea con i più diffusi programmi di posta elettronica utilizzati sia in ufficio che in casa.

Inserendo nell'apposita casella l'indirizzo webmail.infocert.it, si accede alla schermata di Login in cui l'utente deve farsi riconoscere dal sistema attraverso la propria Userid e Password (oppure utilizzare la form nella pagina principale del sito Legalmail come indicato al precedente paragrafo).



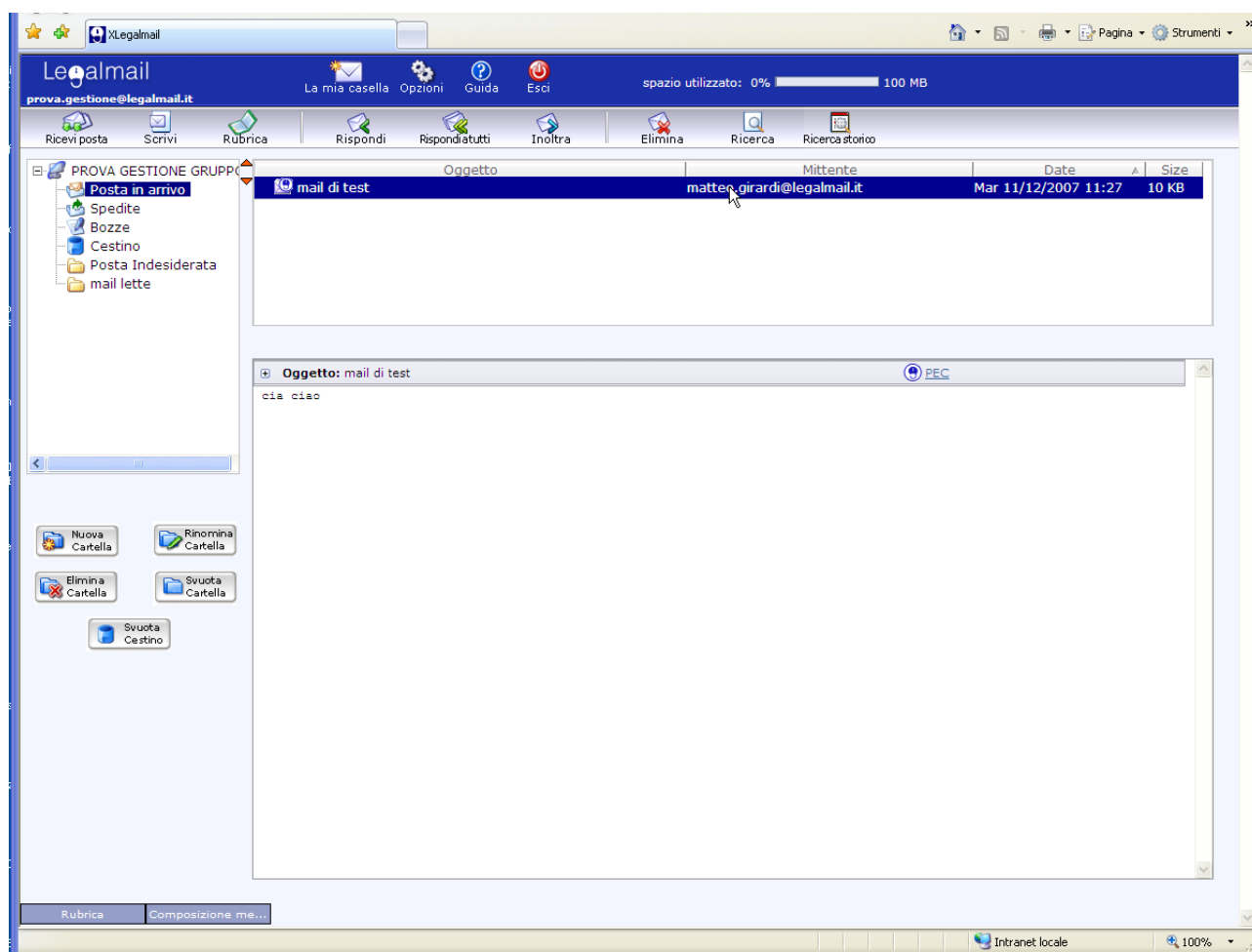
Se l'utente accede per la prima volta a Legalmail, è consigliabile cambiare la password fornita da InfoCert selezionando la voce Cambio Password cliccando il bottone Opzioni (cfr. [Opzioni](#))

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 di Posta Certificata elencato con gli altri servizi da utilizzare.

9.2 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 4 bottoni per le diverse funzioni, a seguire si trova la barra degli strumenti con le funzioni più utilizzate come Ricevi posta, Scrivi, Rispondi ecc. A destra si trova il riquadro relativo alle cartelle e ci si trova posizionati in "Posta in arrivo" Nel riquadro a sinistra (Lista messaggi) si vedono tutti i messaggi contenuti all'interno della cartella selezionata, nel riquadro in basso una descrizione delle caratteristiche di webmail. Non appena si seleziona un messaggio dal riquadro superiore, verrà visualizzato all'interno del riquadro inferiore (anteprima messaggio).



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

9.3 La console

Di seguito viene riportata l'immagine della console che permette di eseguire la configurazione e da informazioni sullo stato della casella



	La mia casella permette di aprire una finestra riepilogativa dei servizi disponibili
	Il bottone opzioni permette di aprire la finestra per la configurazione della casella, dei servizi quali Archivio Storico, Antispam, gestione filtri ecc
	Il bottone guida attiva un help in linea
	Il bottone per uscire dalla webmail

Sul lato destro della barra è presente l'indicatore dello spazio occupato dalla casella.

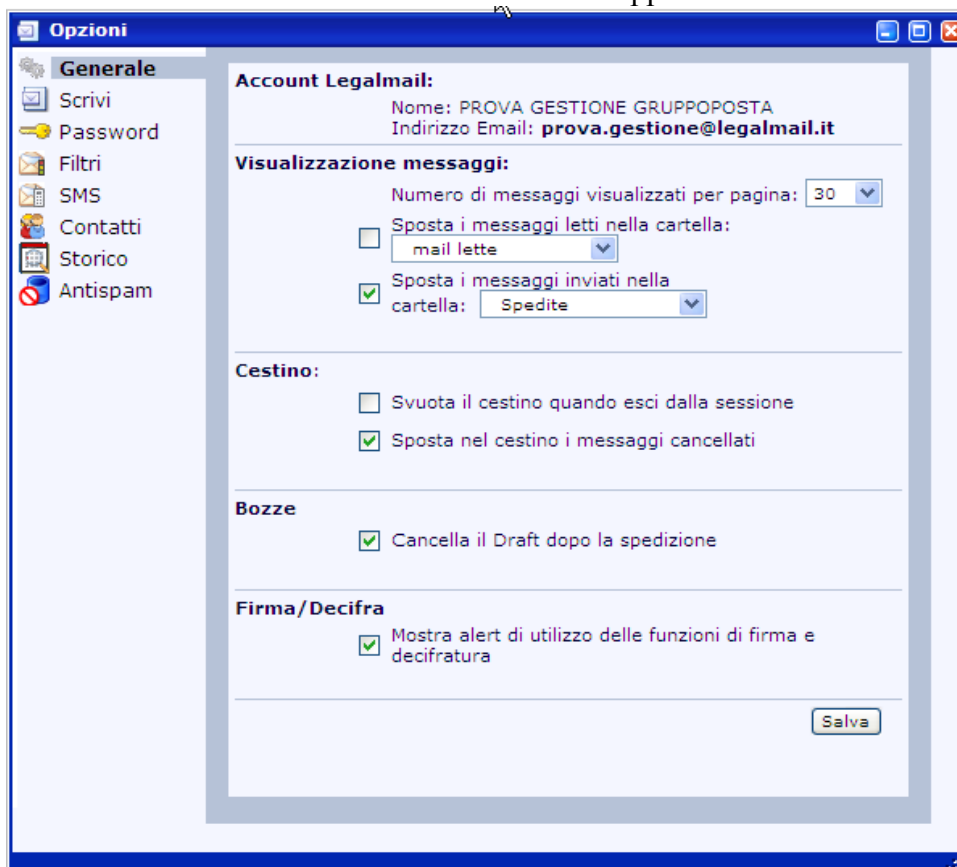
N.B. Per le caselle abilitate ad accedere a più servizi, il link "**cambia**" presente di fianco al nome casella permette di cambiare il tipo di servizio.

9.4 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...

9.4.1 Opzioni: Generale

In questa sezione è possibile personalizzare la gestione dei messaggi: in particolare è possibile spostare messaggi letti in cartelle personalizzate, gestire lo spostamento dei messaggi cancellati nel cestino, cancellarne il contenuto al momento dell'uscita dall'applicazione 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 che l'utente non riesce a cancellare i messaggi.
- L'opzione "Mostra avviso di passaggio a modalità avanzata" consente di visualizzare o meno l'avviso del passaggio alla modalità avanzata.

9.4.2 Opzioni: Scrivi

In questa sezione è possibile personalizzare la composizione di un messaggio inserendo in questo dei testi fissi quali Nome e Cognome, dati riguardanti la denominazione, l'indirizzo, i recapiti della società/persona ecc.

9.4.3 Opzioni: Password

Questa sezione permette di cambiare la password assegnata alla casella.

La nuova password deve contenere da 8 a 20 caratteri, deve contenere almeno un numero e una lettera, non può contenere lo User-ID, non può contenere più di due caratteri uguali consecutivi, deve essere diversa dalle ultime 3 utilizzate in precedenza.

Opzioni

Generale
Scrivi
Password
Filtri
SMS
Contatti
Storico
Antispam

Userid

Password

Nuova Password

Conferma Password

Conferma

Il servizio di cambio password è disponibile nei giorni lavorativi dalle 8.00 alle 21.00
La nuova password deve contenere da 8 a 20 caratteri, deve contenere almeno un numero e una lettera, non può contenere lo user-id, non può contenere più di due caratteri uguali consecutivi, deve essere diversa dalle ultime 3 utilizzate in precedenza

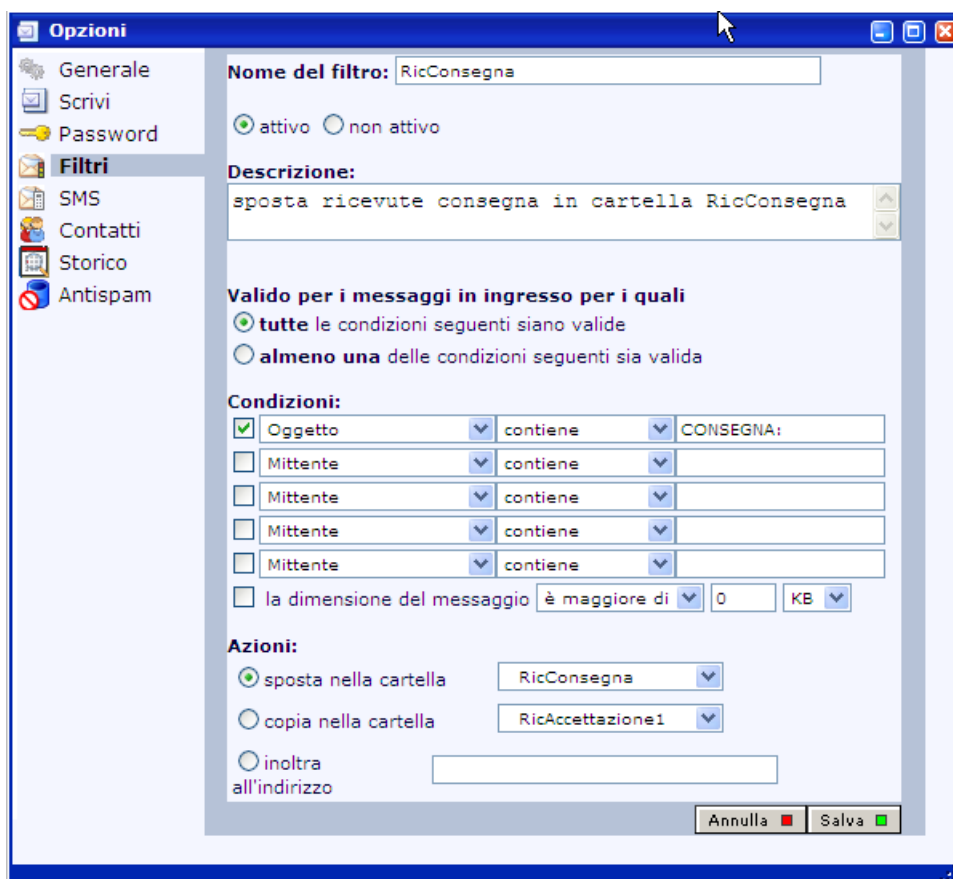
Versione 2.2.7

9.4.4 Opzioni: Filtri

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 posizionarsi nella sezione "Filtri" del menù Opzioni e successivamente premere il bottone "Nuovo": compare la seguente maschera.

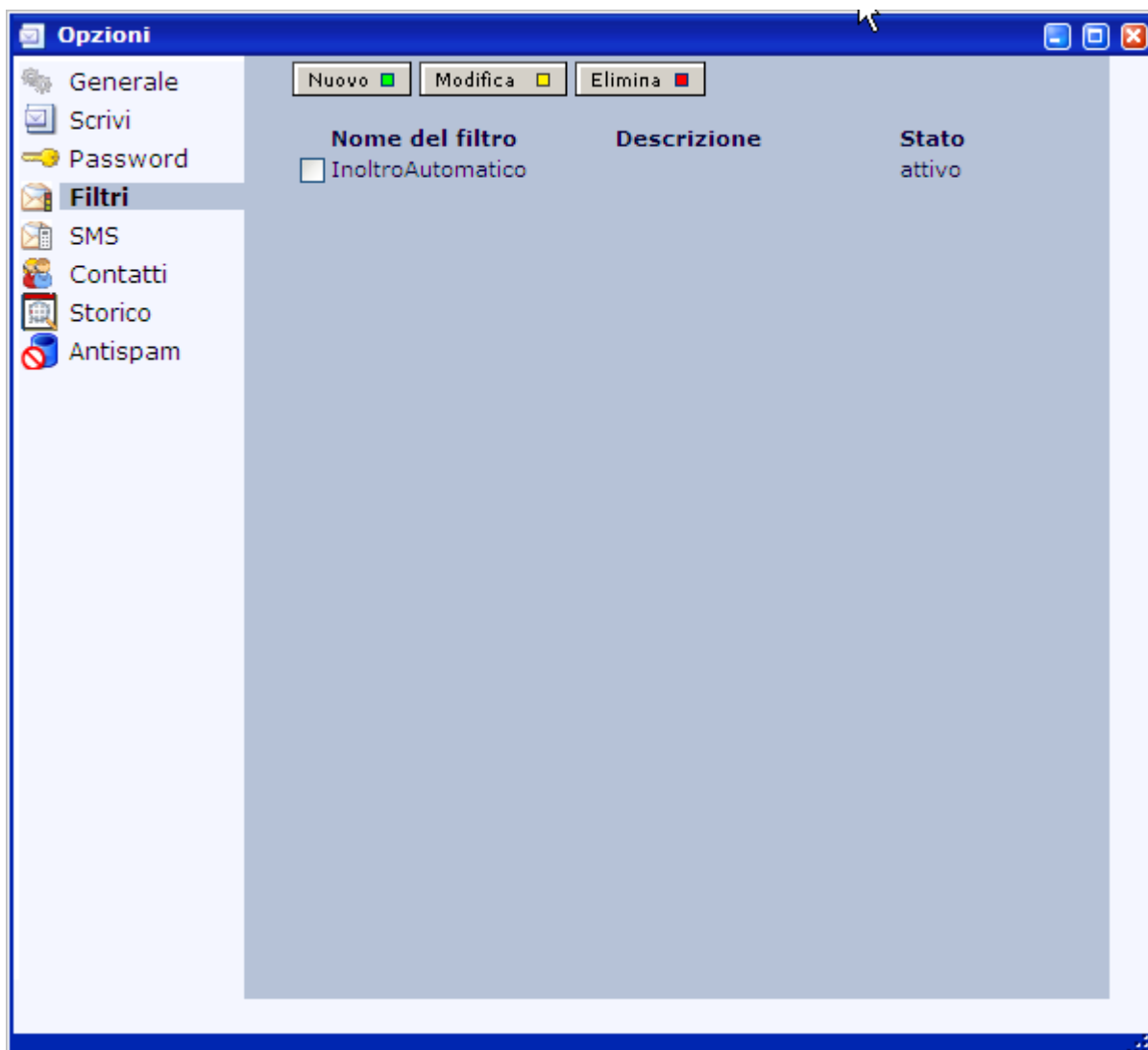


Per esempio: è possibile personalizzare la ricezione di tutte le ricevute di consegna/accettazione in apposite cartelle create dall'utente. Di seguito un esempio di filtro che sposta tutte le ricevute di consegna in una cartella creata dall'utente con il nome di RicConsegna

Per impostare il filtro l'utente deve:

- indicare il nome del filtro (è solo una etichetta);
- impostare il filtro utilizzando la sezione "condizioni"(con l'aiuto degli appositi menù a tendina); le condizioni disponibili sono:
 - testo contenuto nel mittente ('Mittente');
 - testo contenuto nel destinatario diretto ('A');
 - testo contenuto nel destinatario in copia ('CC');
 - testo contenuto in qualsiasi destinatario ('Qualsiasi destinatario');
 - testo contenuto nel subject;
 - dimensione del messaggio, maggiore o minore della quota specificata;
- indicare se le condizioni impostate devono essere tutte soddisfatte o se almeno una delle condizioni deve essere soddisfatta;
- indicare l'Azione; le azioni disponibili sono:
 - sposta in una cartella: il messaggio non viene depositato in "Posta in arrivo", bensì nella cartella indicata (ATTENZIONE: nel caso si utilizzi un client in modalità POP3 il messaggio non sarà più scaricabile in quanto non presente nella casella "Posta in arrivo");
 - copia nella cartella: il messaggio verrà copiato nella cartella indicata oltre che depositato in "Posta in arrivo";
 - inoltra a: vedi sezione successiva per il dettaglio
- 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.

Inoltro automatico

La funzionalità di inoltro automatico dei messaggi in ingresso viene realizzata attraverso la definizione di uno o più filtri (vedi sezione precedente) in cui l'azione specificata sia "Inoltra a".

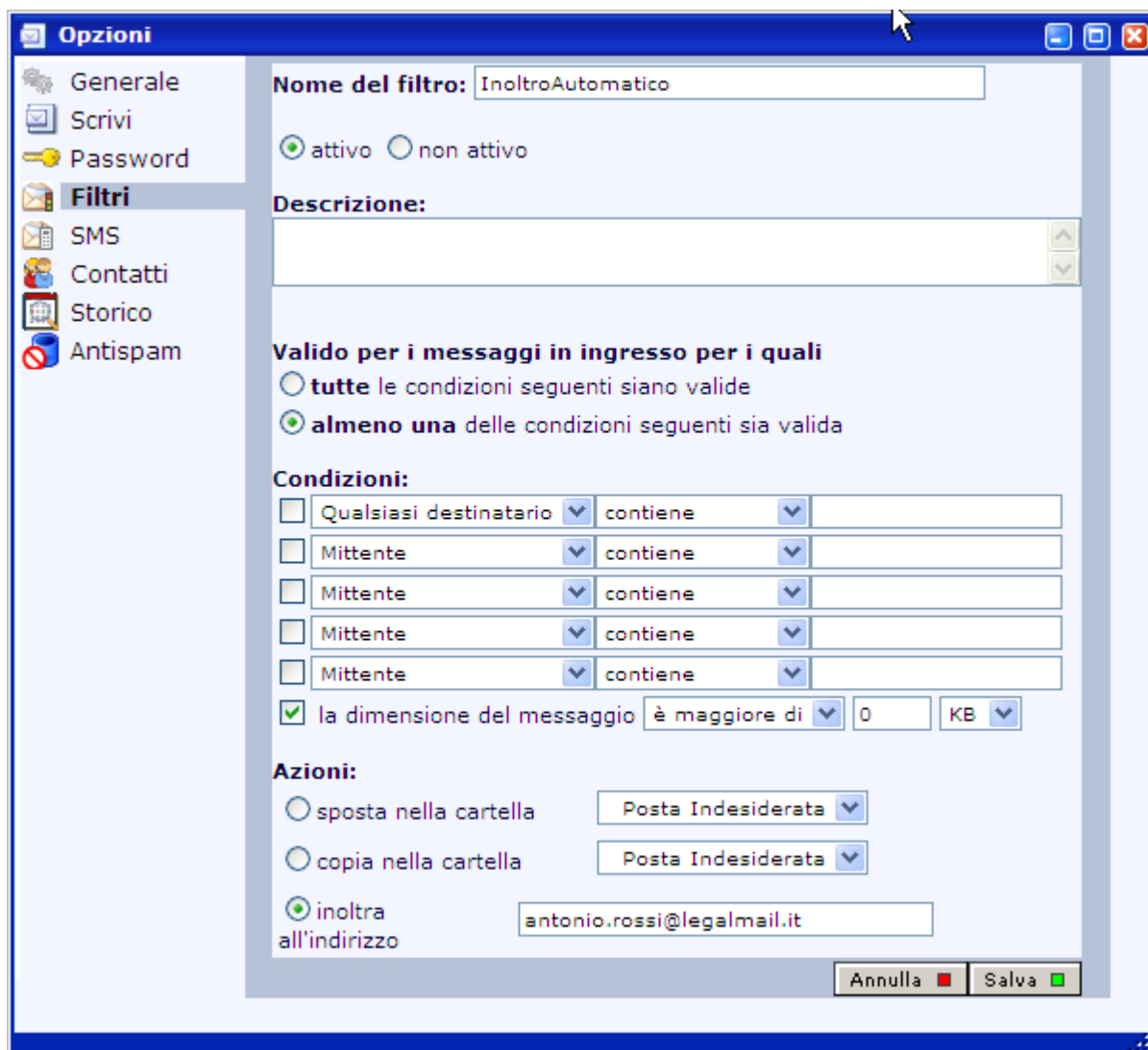
Il messaggio verrà inoltrato alla casella indicata (che può essere certificata oppure non certificata) oltre che depositato in "Posta in arrivo".

ATTENZIONE: l'inoltro viene effettuato dalla casella destinataria del messaggio originale alla casella di inoltro con un invio certificato a nome di chi ha richiesto l'inoltro automatico: per ogni inoltro verrà quindi restituita una ricevuta di accettazione e, nel caso la casella di inoltro sia certificata, una ricevuta di consegna.

NON vengono inoltrati i messaggi relativi a ricevute (di accettazione e di consegna) o errori derivati da invii non correttamente effettuati, questo per evitare problemi di inoltri ripetuti.

Affinché vengano inoltrati tutti i messaggi, si consiglia di selezionare la condizione "dimensione del messaggio" impostandola a maggiore di 0. Agendo invece sull'oggetto del messaggio è possibile distinguere l'inoltro delle mail certificate (impostare "POSTA CERTIFICATA") dalle anomalie (impostare "ANOMALIA MESSAGGIO").

Di seguito viene riportato un esempio di creazione di filtro per inoltro automatico a una casella PEC.



9.4.5 Opzioni: SMS

Questa funzionalità permette la configurazione e attivazione del servizio di notifica tramite SMS. E' necessario essere abilitati al servizio per accedere a questa sezione.

Il servizio prevede l'invio di un messaggio SMS ad un telefono cellulare in caso ci siano messaggi di posta elettronica certificata non letti. La notifica viene inviata una volta al giorno in una fascia oraria stabilita dall'utente.

La notifica avverte della presenza dei soli messaggi in arrivo da utenti di posta certificata; l'avviso non viene inviato in presenza di ricevute (accettazione o consegna) o messaggi di anomalia non letti.

Le opzioni permettono di definire:

- numero di telefono a cui inviare il messaggio
- orario in cui si preferisce l'invio dell'SMS di notifica.
- lo stato del servizio (attivo/non attivo); è possibile sospendere il servizio

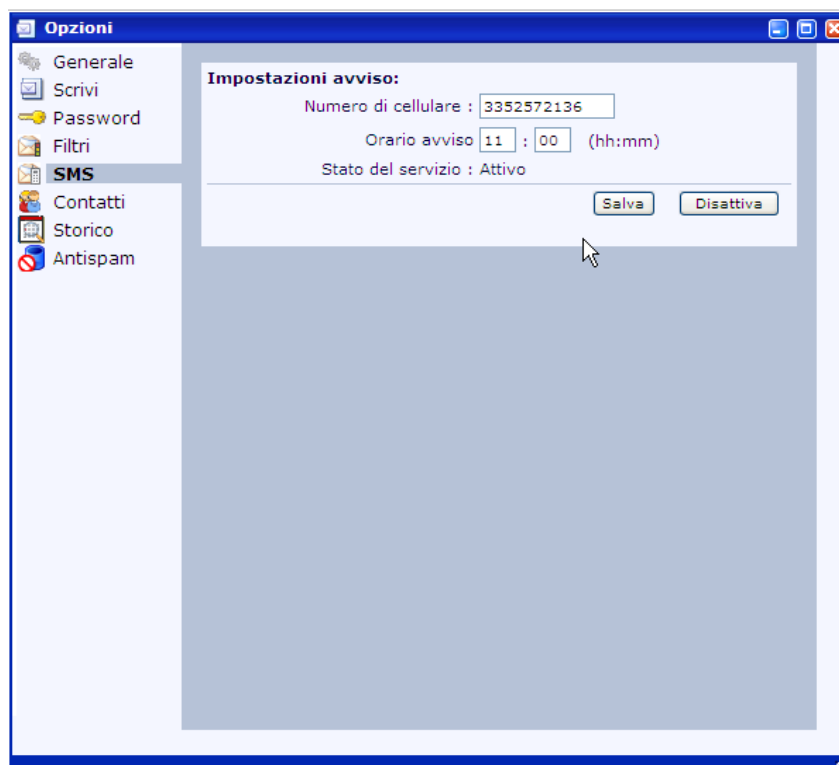
Attivazione del servizio

Una volta abilitati al servizio è necessario procedere alla attivazione del servizio, configurando opportunamente l'orario di ricezione e il numero di telefono.

Alla prima configurazione (attivazione) il servizio procede all'invio di un messaggio di verifica al numero di cellulare indicato dall'utente.

Per completare la procedura è necessario che l'utente risponda al messaggio ricevuto seguendo le indicazioni all'interno del messaggio stesso.

Conclusa la procedura di attivazione il servizio procede all'invio della notifica di posta non letta nell'orario stabilito.



In particolare va inserito il numero di cellulare a cui far pervenire l'sms di notifica e l'orario in cui eseguire il controllo. Questo servizio avvisa solo se nella casella sono presenti messaggi non ancora letti provenienti da indirizzi di posta certificati.

N.B. Perché l'attivazione vada a buon fine il servizio invierà un primo sms al quale bisognerà rispondere inserendo nel testo del messaggio LMCA SI

9.4.6 Opzioni: Contatti

Questa sezione permette di inoltrare una mail con le osservazioni direttamente ad una casella gestita dal servizio di Call Center.

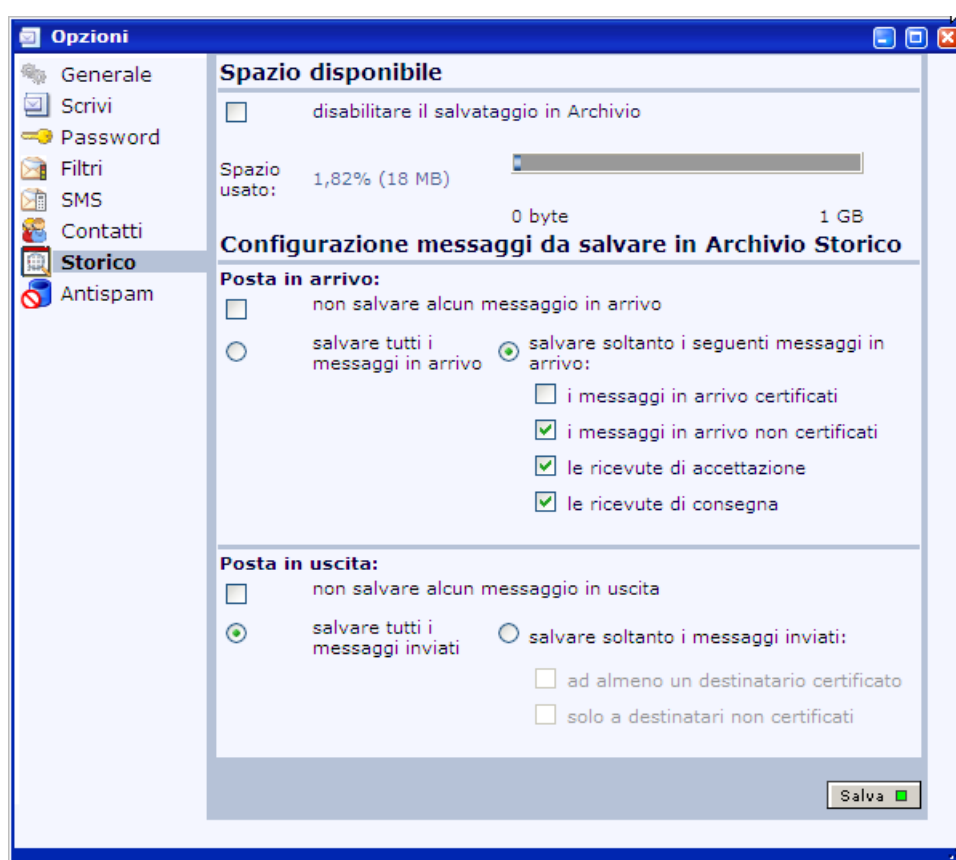
9.4.7 Opzioni: Storico

La normativa impone ad InfoCert, quale gestore del servizio di Posta Certificata, di tenere traccia per trenta mesi dei messaggi in entrata ed uscita dal sistema. Tale obbligo, tuttavia, non si estende al contenuto dei messaggi.

InfoCert mette quindi a disposizione, a pagamento, il servizio di Archivio Storico, con il quale i messaggi in transito nelle caselle di Posta Elettronica Certificata possono essere salvati in modo sicuro e trasparente per l'utente.

Dopo aver acquistato il servizio ed essere stati abilitati è necessario attivare il servizio di Archivio Storico accedendo alla casella di Posta Certificata attraverso il sito www.legalmail.it.

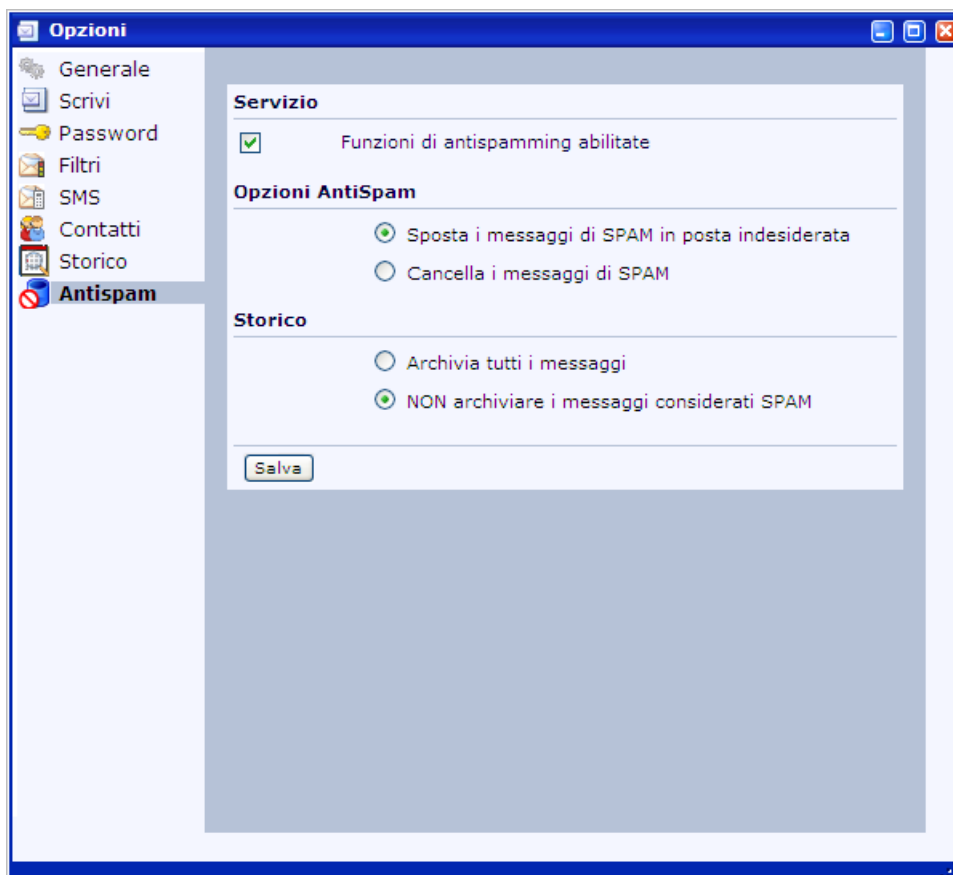
Per abilitare tale funzione togliere il flag “disabilitare il salvataggio in Archivio”, impostare la modalità di archiviazione dei messaggi desiderata:



- scegliere le categorie di messaggi da salvare:
 - posta in arrivo:
 - messaggi certificati (ovvero provenienti da un indirizzo di Posta Certificata);
 - messaggi non certificati (ovvero provenienti da un indirizzo di posta tradizionale);
 - ricevuta di accettazione (compresi gli avvisi di mancata accettazione);
 - ricevute di consegna (compresi gli avvisi di mancata consegna);
 - posta in uscita:
 - messaggi destinati ad almeno un destinatario certificato;
 - messaggi destinati solo ad indirizzi non certificati.

9.4.8 Opzioni: Antispam

Il bottone “**opzioni**” permette di attivare la finestra sottostante dalla quale si possono personalizzare funzioni aggiuntive quali Archivio Storico, SMS e Antispam.



Attivare il flag *Funzioni di antispamming abilitate*.

Ci sono due modalità di gestione dello spam:

- *Spostare i messaggi di spam in “posta indesiderata”* In questa modalità i messaggi di spam vengono automaticamente intercettati e spostati in una cartella ad hoc chiamata Posta Indesiderata che dovrà essere gestita manualmente. Verranno spostati su questa cartella tutti i messaggi riconosciuti come *spam* (il punteggio di spam è alto), *suspected spam* (il punteggio di spam è intermedio), *blocked sender* (l'indirizzo del mittente o l'indirizzo ip utilizzato per l'invio è riconosciuto come spam).
- *Cancellare i messaggi di SPAM* In questa modalità i messaggi di spam riconosciuti come tali dal sistema saranno automaticamente cancellati. Quelli riconosciuti come *suspected spam* oppure *blocked sender* saranno invece spostati in “Posta indesiderata”.

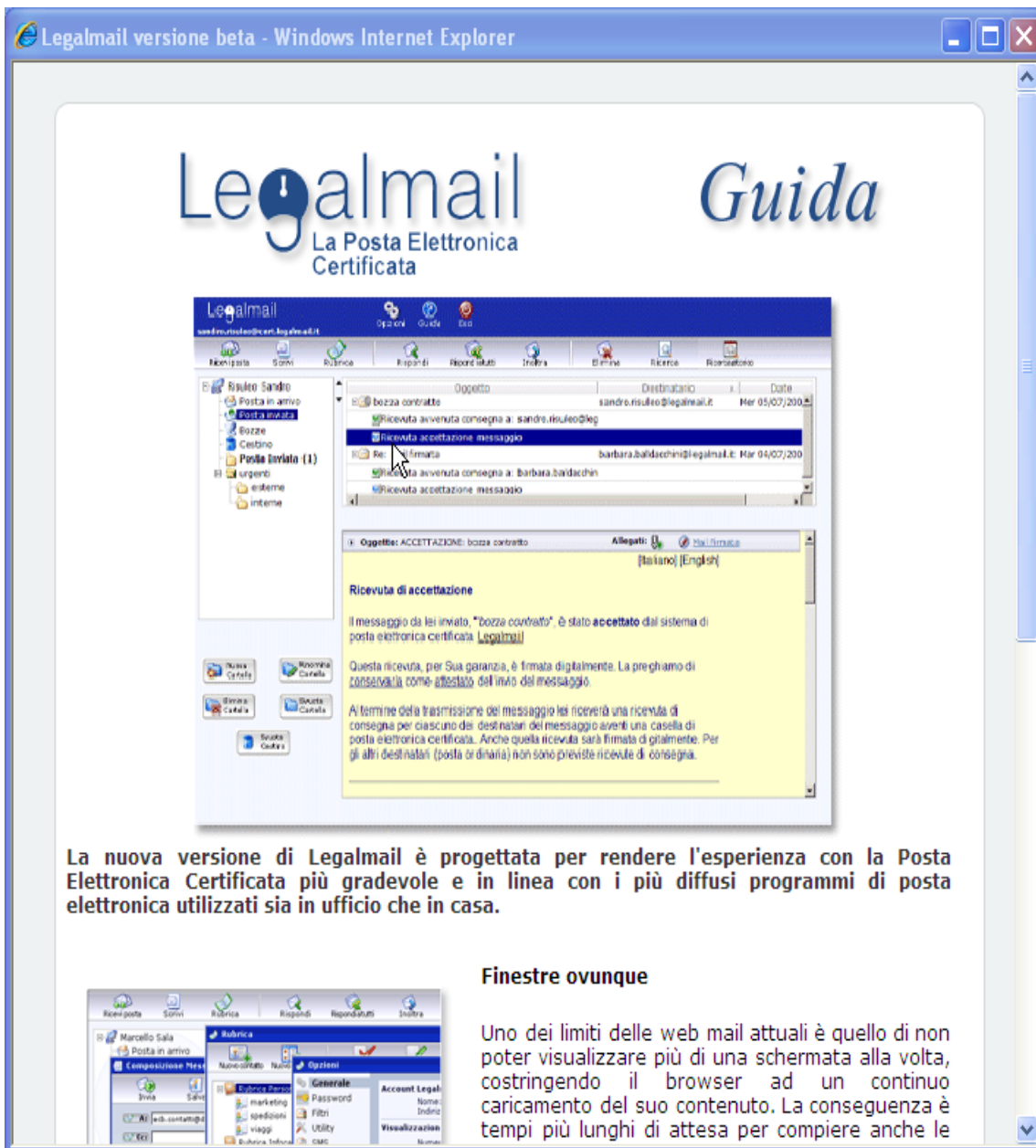
Per ogni modalità è possibile gestire

- Spostare i messaggi in “Posta indesiderata” e mantenerne una copia in archivio storico
- Spostare i messaggi in “Posta Indesiderata” senza mantenerne una copia in archivio storico
- Cancellare i messaggi di SPAM dopo averne salvata una copia in archivio storico
- Cancellare i messaggi di SPAM senza salvarne una copia in archivio storico (in quest'ultimo caso non sarà più possibile recuperare il messaggio)

Una volta impostata la configurazione desiderata cliccare sul bottone **salva**.

9.5 Guida:

Il bottone guida permette di aprire la finestra “Guida in linea”



La nuova versione di Legalmail è progettata per rendere l'esperienza con la Posta Elettronica Certificata più gradevole e in linea con i più diffusi programmi di posta elettronica utilizzati sia in ufficio che in casa.

Finestre ovunque

Uno dei limiti delle web mail attuali è quello di non poter visualizzare più di una schermata alla volta, costringendo il browser ad un continuo caricamento del suo contenuto. La conseguenza è tempi più lunghi di attesa per compiere anche le

10. Barra degli strumenti

La barra degli strumenti consente di attivare le funzioni più comuni di un sistema di posta quali ricezione, scrittura, risposta ecc.



10.1 descrizione delle funzioni



Permette di controllare se in casella sono presenti nuovi messaggi: se presenti aggiorna il contenuto della finestra messaggi



Permette di attivare la finestra di composizione di un messaggio



Attiva la finestra per la gestione della rubrica personale



Permette di aprire la finestra di composizione messaggio con i dati del destinatario a cui si vuole rispondere (i destinatari in CC non vengono inseriti)



Come sopra ma compila anche il capo CC



Apri la finestra di composizione messaggio e permette di inoltrare il messaggio ad un nuovo destinatario



Elimina dall'elenco i messaggi selezionati; i messaggi vengono spostati nella cartella cestino (o in quella selezionata attraverso il menù opzioni, cfr. [Opzioni](#)); è possibile eliminare un messaggio anche trascinandolo direttamente dentro la cartella cestino dalla finestra dei messaggi.



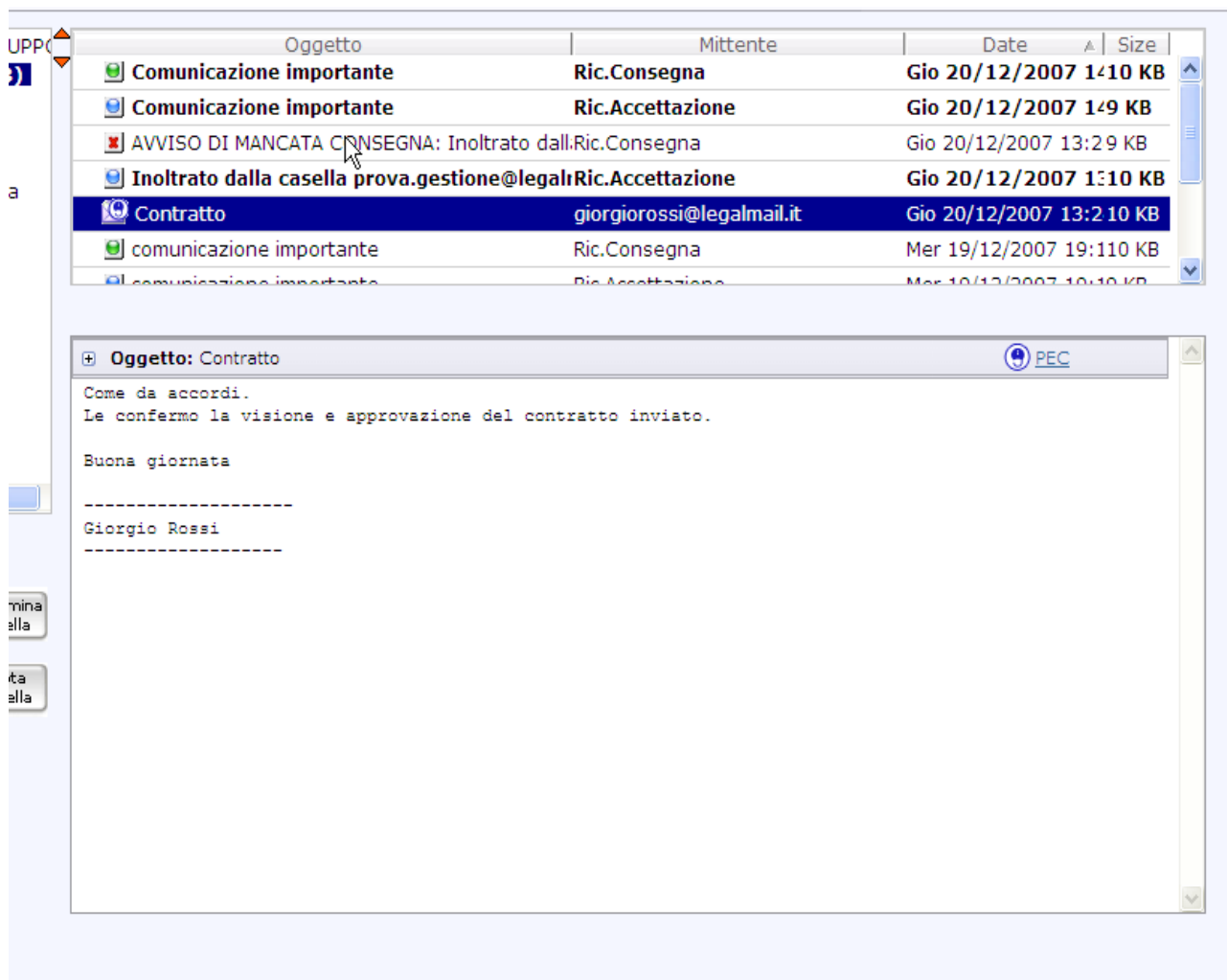
Consente l'apertura della finestra per la ricerca dei messaggi. E' possibile inserire alcuni parametri di ricerca. L'esito delle ricerca viene proposto nella finestra dei messaggi.



Attiva la modalità di ricerca in archivio storico. Compare la maschera di inserimento delle informazioni da ricercare.

11. Lista dei messaggi e anteprima

Di seguito viene riportata l'immagine relativa all'area relativa alla lista dei messaggi e all'anteprima del messaggio



The screenshot shows an email client interface with a list of messages and a preview pane. The list has columns for 'Oggetto', 'Mittente', 'Date', and 'Size'. The preview pane shows the content of the selected message.

Oggetto	Mittente	Date	Size
Comunicazione importante	Ric.Consegna	Gio 20/12/2007 14:10	10 KB
Comunicazione importante	Ric.Accettazione	Gio 20/12/2007 14:9	KB
AVVISO DI MANCATA CONSEGNA: Inoltrato dall.	Ric.Consegna	Gio 20/12/2007 13:29	KB
Inoltrato dalla casella prova.gestione@legal	Ric.Accettazione	Gio 20/12/2007 13:10	KB
Contratto	giorgiorossi@legalmail.it	Gio 20/12/2007 13:2	10 KB
comunicazione importante	Ric.Consegna	Mer 19/12/2007 19:11	10 KB
comunicazione importante	Ric.Accettazione	Mer 19/12/2007 19:10	KB


Oggetto: Contratto

Come da accordi.
 Le confermo la visione e approvazione del contratto inviato.

Buona giornata

 Giorgio Rossi








è possibile ordinare i messaggi secondo l'oggetto, il mittente, la data semplicemente cliccando il bottone corrispondente nell'area della lista. Selezionando con un click il messaggio, nell'area dell'anteprima apparirà il contenuto. Se si clicca 2 volte col mouse sopra il messaggio, questo si apre in una nuova finestra con funzionalità avanzate per la gestione dello stesso.

Le freccette  consentono di ridimensionare le due aree secondo le esigenze dell'utilizzatore.

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.

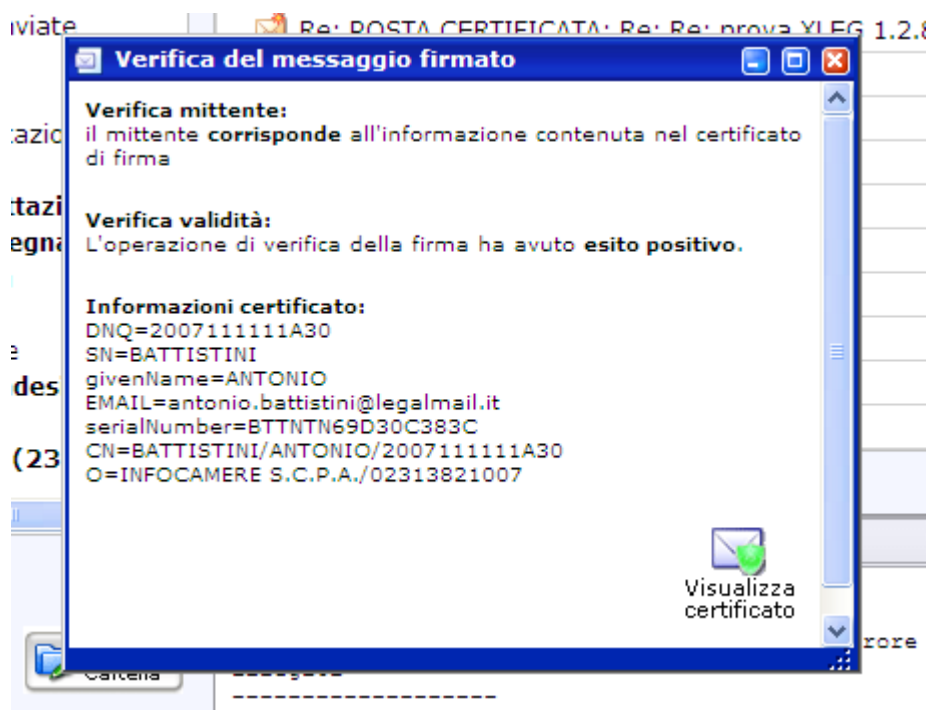
Sul lato sinistro di ogni messaggio è presente un'icona che definisce il tipo di messaggio visualizzato. Di seguito una tabella con le varie tipologie

11.1 Tipologie dei messaggi


	Messaggio proveniente da posta certificata e firmato digitalmente
	Messaggio proveniente da posta certificata
	Messaggio proveniente da indirizzo mail non certificato
	Messaggio crittografato
	Ricevuta di consegna
	Ricevuta di accettazione
	Ricevuta di mancata consegna


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).

Cliccando sul bottone raffigurante una penna (Mail firmata), 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).

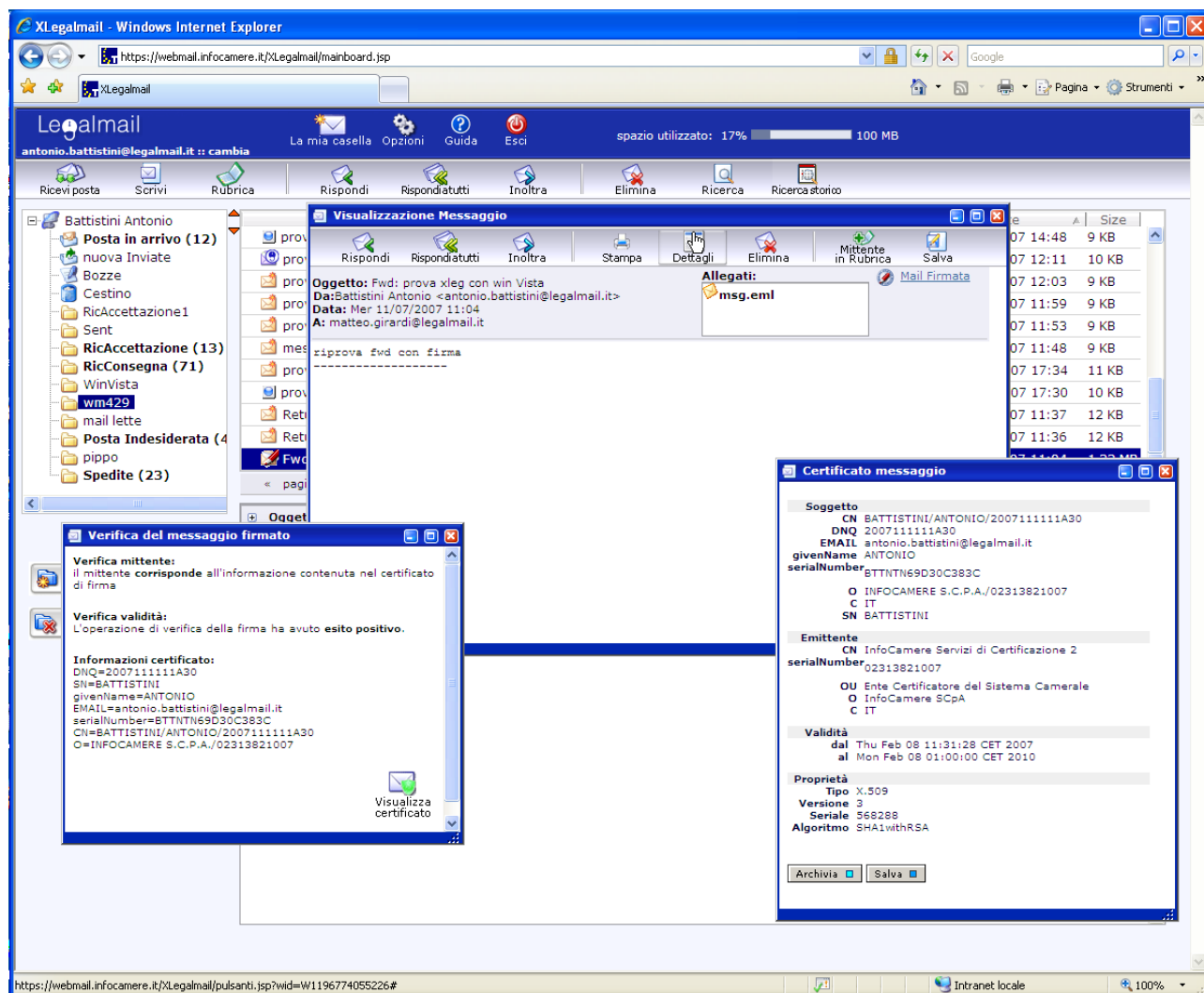


Se si preme il bottone “Visualizza certificato” appare una finestra con i dati completi relativi al certificato di firma.

il bottone  consente di salvare il certificato nella sezione Certificati (per inviare un messaggio crittografato è necessario aver ricevuto un messaggio firmato digitalmente dal

destinatario)mente se si clicca  il certificato chiamato "cert.cer" verrà salvato sul disco locale

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


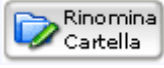

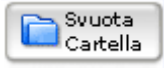



Se su un messaggio nella lista si clicca due volte col mouse comparirà una finestra per la visualizzazione e la gestione del messaggio: ogni messaggio, a seconda della sua tipologia, è costituito da alcune parti fisse descrittive, dagli allegati di posta certificata e dagli allegati al messaggio (alcuni esempi di messaggi di posta certificata sono consultabili al par. [Esempi di messaggi di posta certificata](#)).

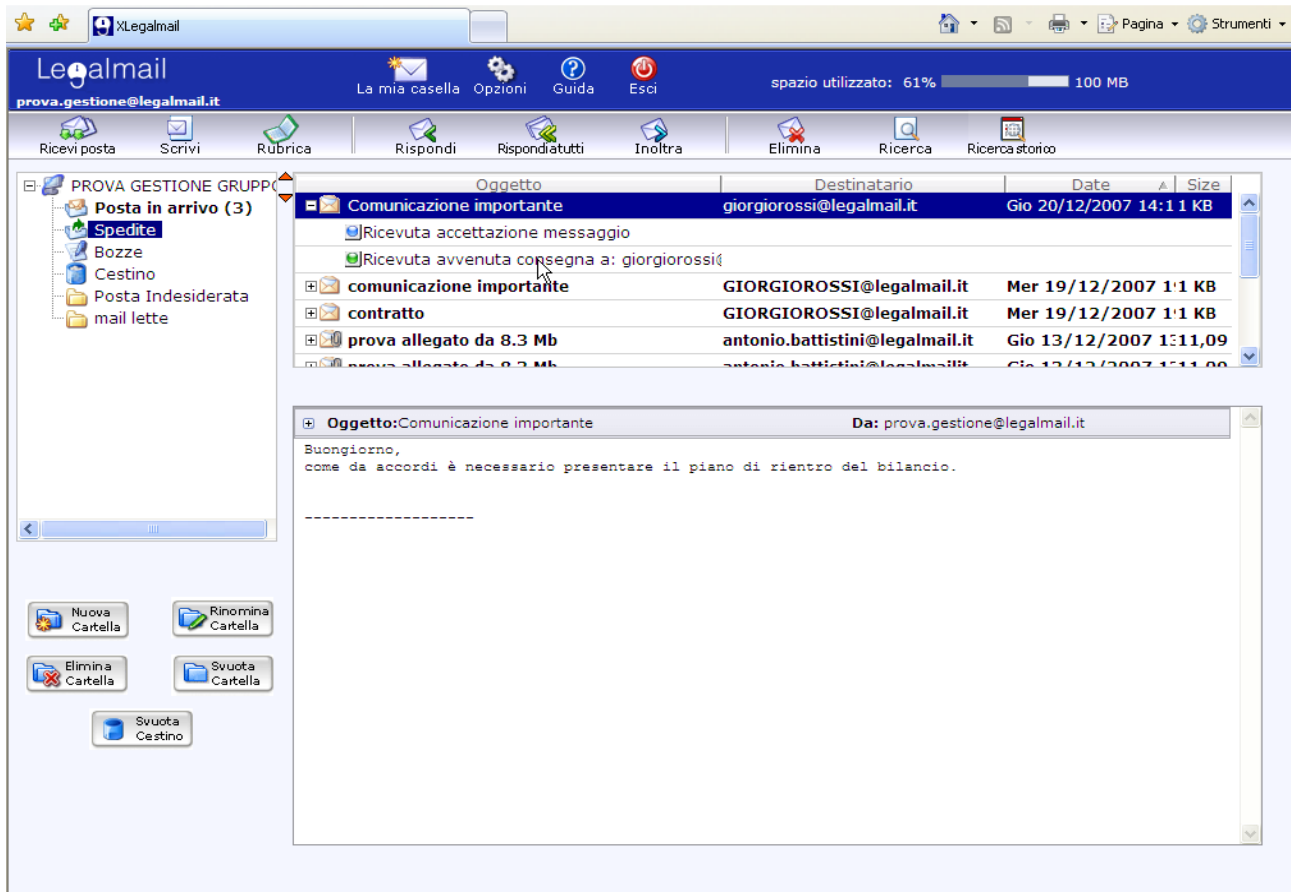
Nel caso il messaggio sia stato crittografato è necessario utilizzare la modalità avanzata: se l'utente sta utilizzando la modalità normale un messaggio lo avvisa di passare all'altra modalità (cfr. [Ricezione di messaggi crittografati](#))

12. Gestione cartelle

L'area in alto a sinistra visualizza tutte le cartelle relative all'indirizzo di posta. E' possibile spostarsi da una cartella all'altra semplicemente cliccandoci sopra. L'area "Lista dei messaggi" cambia il suo contenuto in funzione della cartella selezionata. I bottoni permettono infine le seguenti azioni:

	Permette la creazione di una nuova cartella a partire dalla cartella in cui ci si trova posizionati
	Permette di rinominare la cartella in cui si è posizionati
	Elimina la cartella in cui si è posizionati ATTENZIONE: se la cartella contiene messaggi anche questi verranno cancellati
	Cancella i messaggi contenuti nella cartella
	Svuota la cartella Cestino

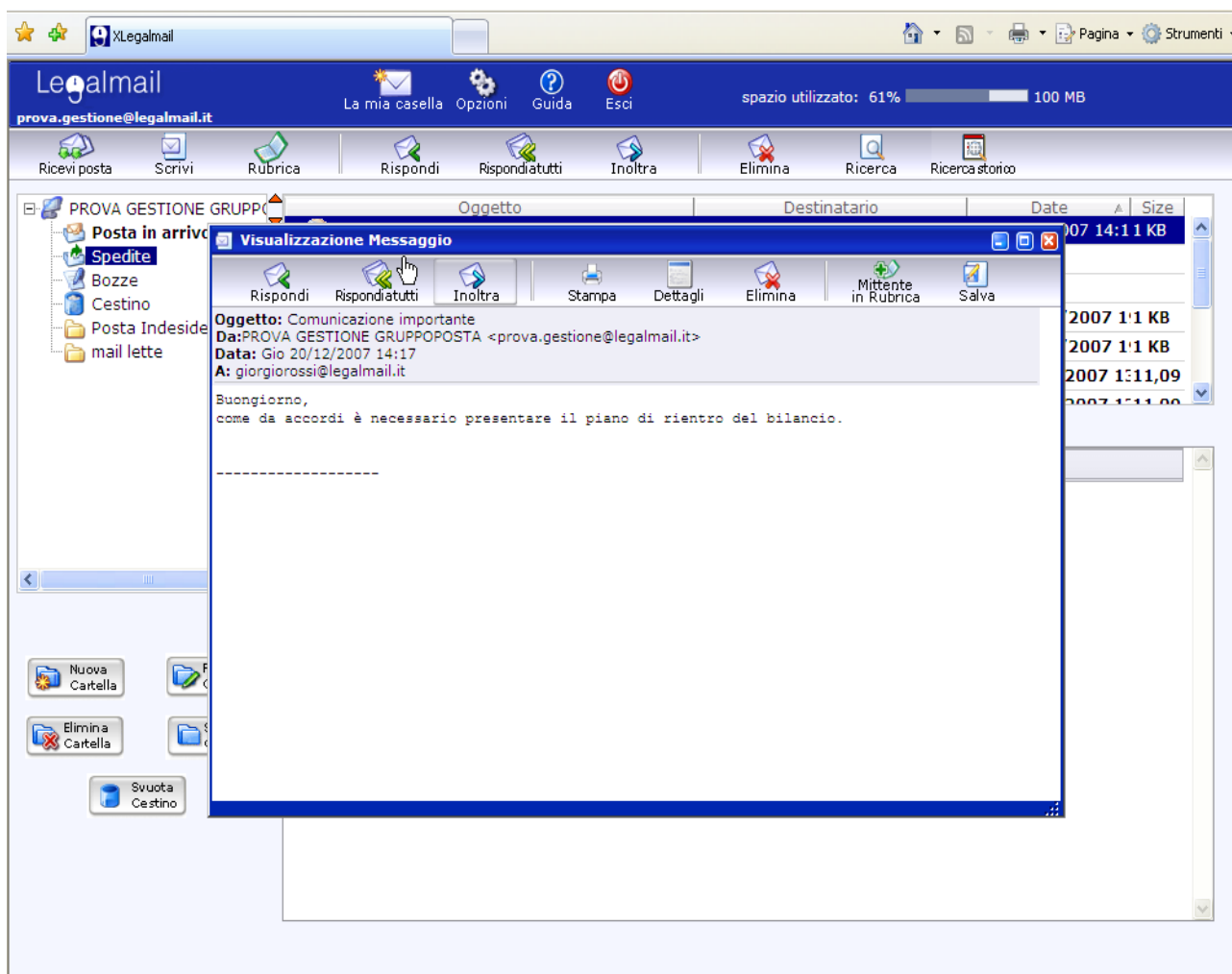
N.B. Se ci si posiziona nella cartella dei messaggi inviati, nella lista dei messaggi vengono evidenziati tutti i messaggi e se si clicca sul simbolo del + che sta sul lato sinistro del messaggio vengono raggruppate ed evidenziate tutte le ricevute relative all'invio del messaggio






The screenshot shows the Legalmail web interface. At the top, there's a navigation bar with 'La mia casella', 'Opzioni', 'Guida', and 'Esci'. Below that, a toolbar contains icons for 'Ricevi posta', 'Scrivi', 'Rubrica', 'Rispondi', 'Rispondiatutti', 'Inoltra', 'Elimina', 'Ricerca', and 'Ricerca storico'. The main area is divided into a left sidebar with a folder tree (PROVA GESTIONE GRUPPO, Posta in arrivo (3), Spedite, Bozze, Cestino, Posta Indesiderata, mail lette) and a central message list. The message list has columns for 'Oggetto', 'Destinatario', 'Date', and 'Size'. The selected message is 'Comunicazione importante' from 'giorgiorossi@legalmail.it' dated 'Gio 20/12/2007 14:11 KB'. Below the list, the message content is visible, starting with 'Buongiorno, come da accordi è necessario presentare il piano di rientro del bilancio.' At the bottom left, there are five icons for mailbox management: 'Nuova Cartella', 'Rinomina Cartella', 'Elimina Cartella', 'Svuota Cartella', and 'Svuota Cestino'.


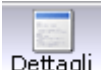


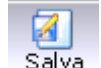
13. La finestra “Visualizzazione messaggio”

La finestra di visualizzazione messaggio si apre sopra la finestra principale di Legalmail ed è possibile spostarla all'interno dell'area di Legalmail semplicemente cliccando e tenendo premuto il bottone sinistro del mouse. E' possibile inoltre aprire più finestre di visualizzazione contemporaneamente, trascinarle all'interno dell'area, ridurle ad icona per richiamarle successivamente. La finestra si presenta come in figura e all'interno sono presenti i bottoni per la gestione del messaggio stesso.

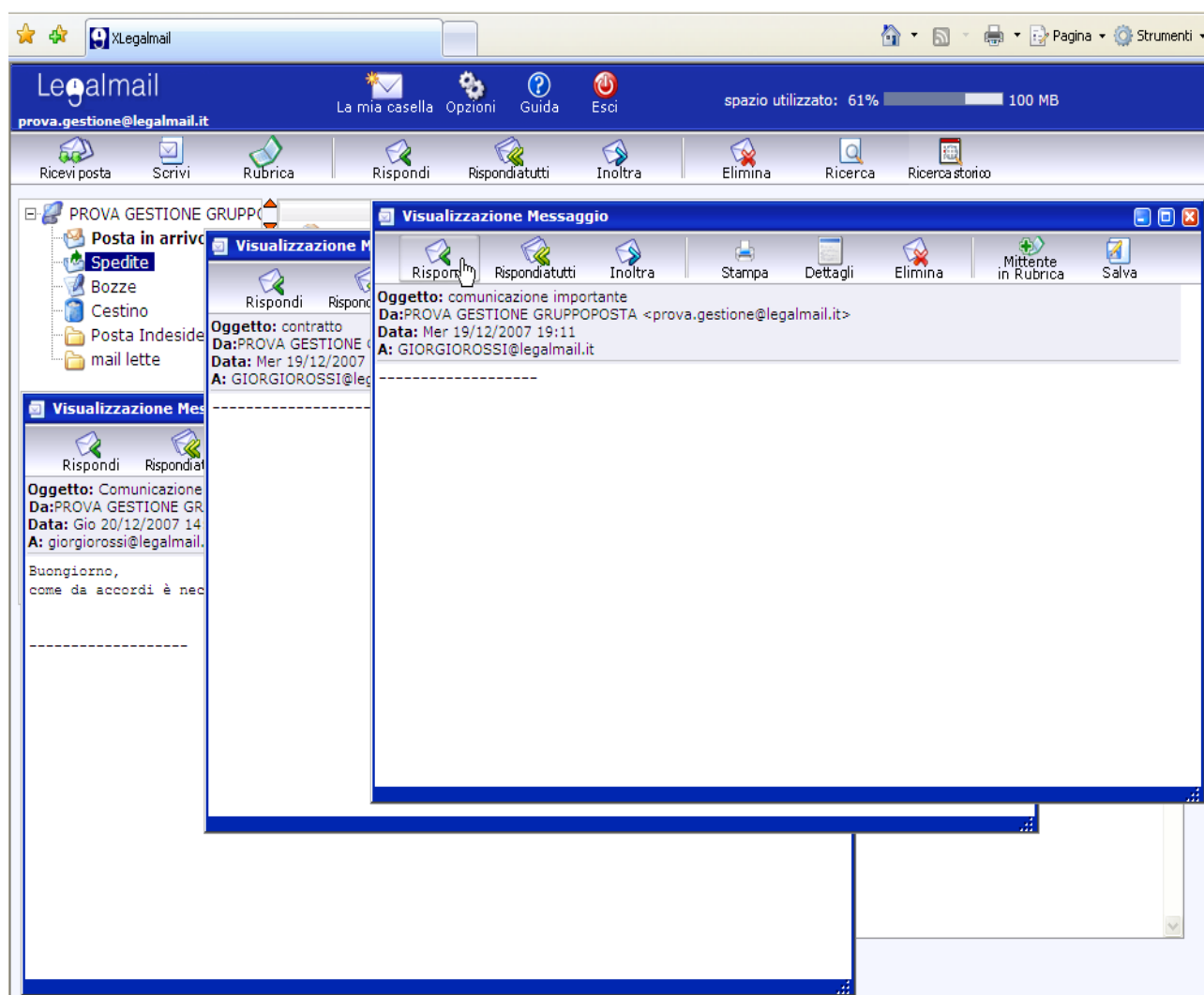


La tabella sottostante illustra le funzioni della barra dei bottoni per la finestra di visualizzazione messaggio

	Compare la finestra di composizione Nuovo messaggio per rispondere al mittente Vengono già precompilati alcuni campi del messaggio.(cfr. Nuovo Messaggio)
	Compare la finestra di composizione Nuovo messaggio per rispondere al mittente e a tutti i destinatari. Vengono già precompilati alcuni campi del messaggio.(cfr. Nuovo Messaggio)
	Compare la finestra di composizione Nuovo messaggio con già compilati i campi del messaggio tranne che per il destinatario/i(cfr. Nuovo Messaggio)

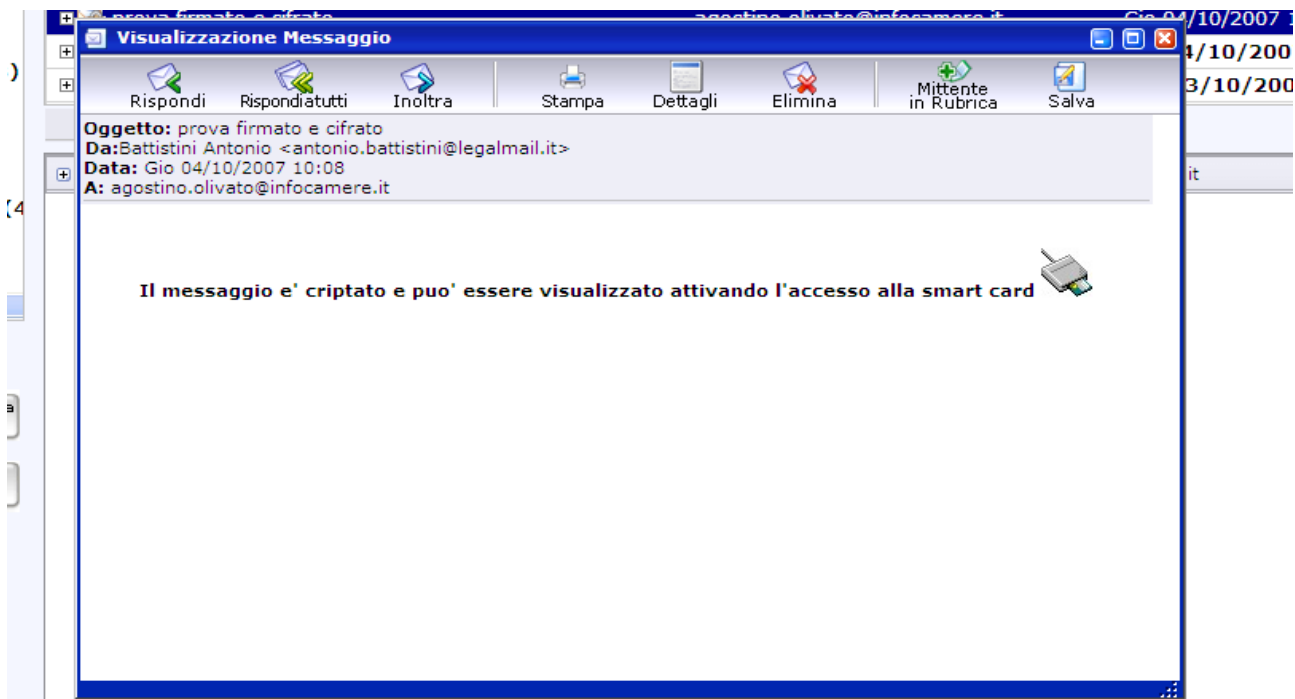
 Stampa	Apre la finestra con i dati del messaggio e il bottone per mandarlo in stampa. Se si clicca sul bottone stampa il messaggio sarà inviato alla stampante.
 Dettagli	Apre una finestra con i dati in formato XML relativi al messaggio
 Elimina	Permette la cancellazione del messaggio
 Mittente in Rubrica	Aggiunge alla rubrica personale il mittente del messaggio. Apre la finestra Nuovo contatto
 Salva	Permette di salvare sul disco locale una copia del messaggio con nome <i>message.eml</i>

Come al solito è possibile aprire più finestre di visualizzazione relative a vari messaggi e poi è possibile passare da una finestra all'altra semplicemente cliccandoci sopra

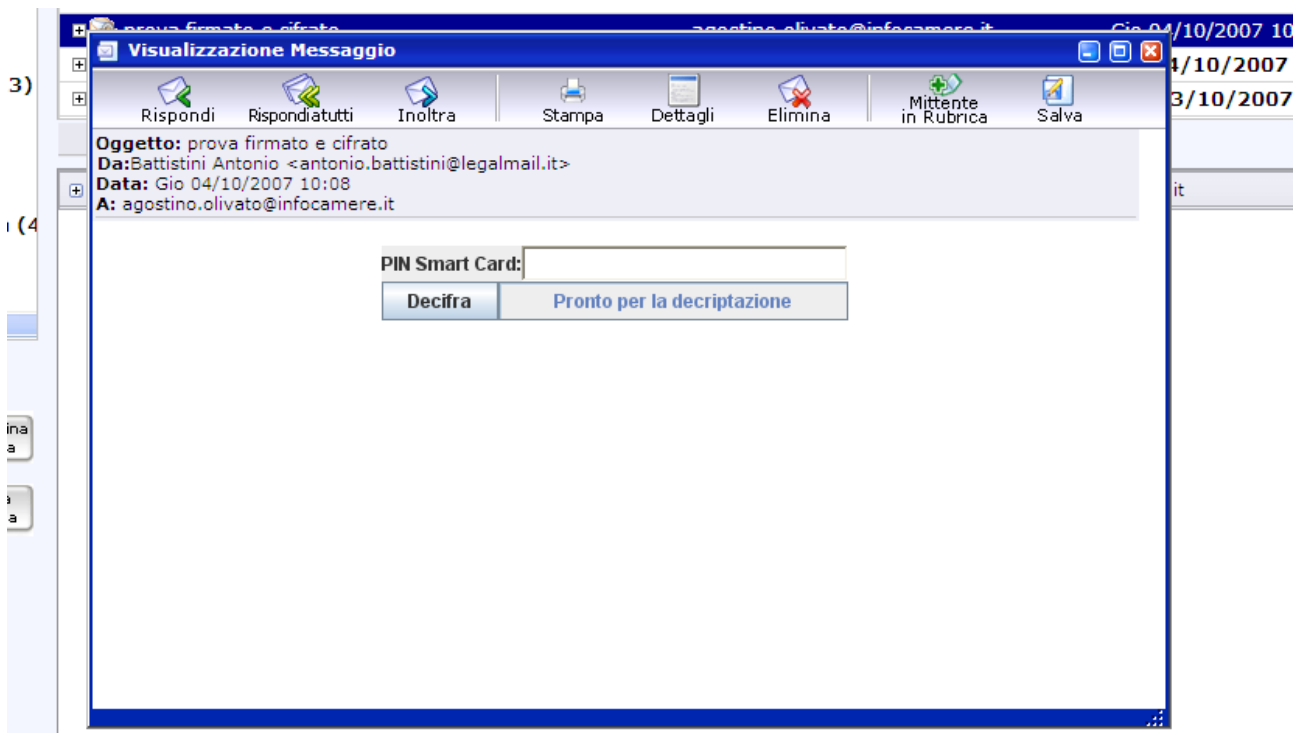


13.1 Ricezione di messaggi crittografati

Se l'utente riceve un messaggio crittografato, quando seleziona il messaggio per leggerlo, comparirà la scritta riportata in figura: cliccando sul link “*accesso alla smart card*”



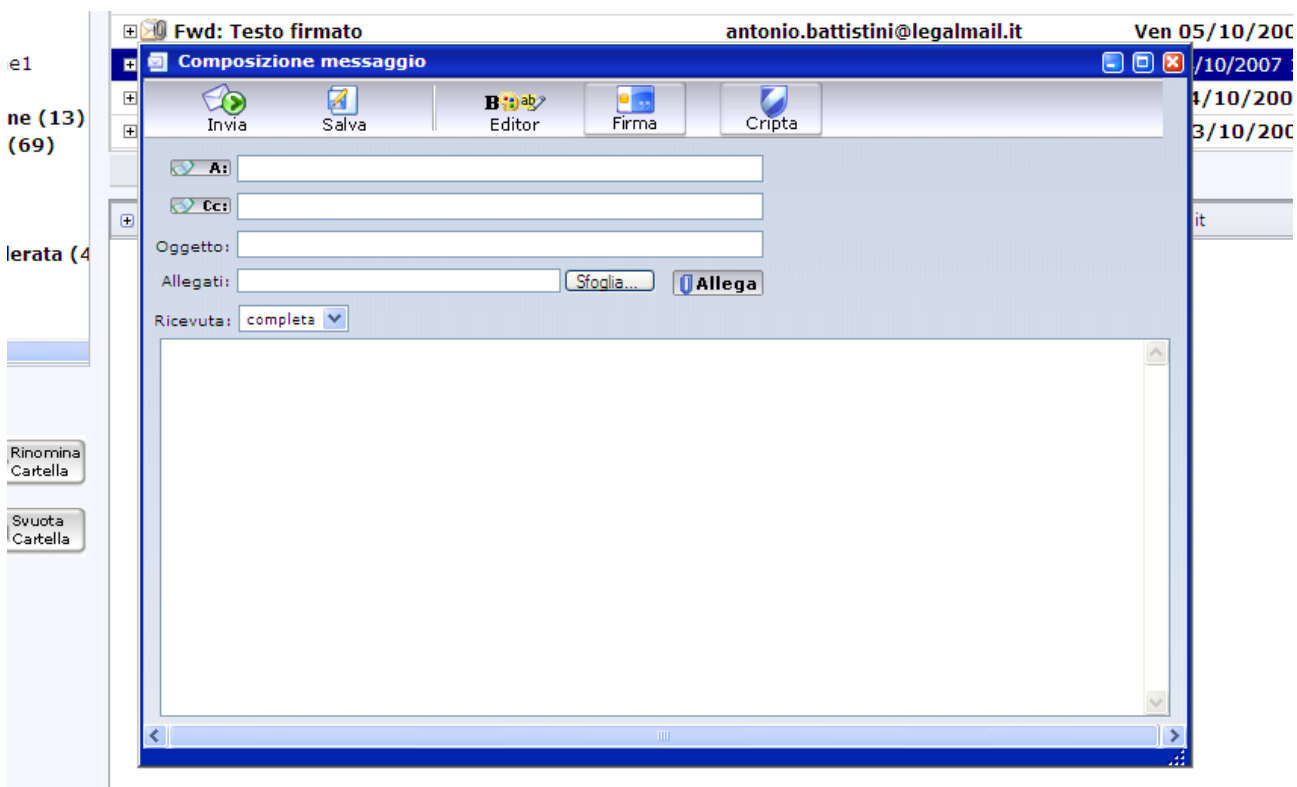
si attiveranno le funzioni per decifrare e verrà richiesto il pin








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).

14. Nuovo Messaggio

Dalla maschera principale cliccare “**Scrivi**”. Si apre la finestra di Composizione messaggio



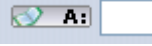
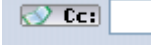
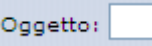
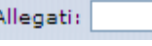
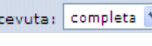
questa finestra permette di comporre un messaggio nuovo da inviare: i bottoni permettono di:

	Permette di inviare il messaggio ai destinatari. Quando si preme il bottone vengono eseguite le operazioni di verifica sul messaggio
	Permette di salvare il messaggio nella cartella Bozze
	Attiva un editor di testo che permette funzioni avanzate per la scrittura dei messaggi
	Bottone che attiva le funzioni di firma. Quando viene premuto, vengono scaricati sul computer dell'utilizzatore dei componenti aggiuntivi (solo la prima volta che si preme). Per permettere questo è necessario permettere al browser che si sta utilizzando il download dei componenti. Una volta premuto, il bottone rimane evidenziato in bianco.
	Bottone che attiva le funzioni di crittografia. Quando viene premuto, vengono scaricati sul computer dell'utilizzatore dei componenti aggiuntivi (solo la prima volta che si preme). Per permettere questo è necessario permettere al browser che si sta utilizzando il download dei componenti. Una volta premuto, il bottone rimane evidenziato in bianco.

Per usufruire dei servizi di firma digitale e crittografia è necessario che l'utente abbia una smartcard InfoCert 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).

14.1 Descrizione dei campi:

	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;
	Digitare in questo campo l'oggetto del messaggio
	Il tasto Sfogli a 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 Allega . Il documento sarà inserito in una nuova finestra dove vengono elencati i documenti allegati. Il link Rimuovi permette di togliere l'allegato.
	Permette di scegliere il tipo di ricevuta.

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 nel caso l'utente abbia settato l'opzione di salvataggio dei messaggi inviati (cfr. [Opzioni](#)) e il messaggio non possa essere salvato nella cartella dei messaggi inviati perché la dimensione supera lo spazio libero in casella.

Per attivare le modalità di firma e di crittografia è sufficiente cliccare sui relativi bottoni che si evidenzieranno in funzione della loro pressione.

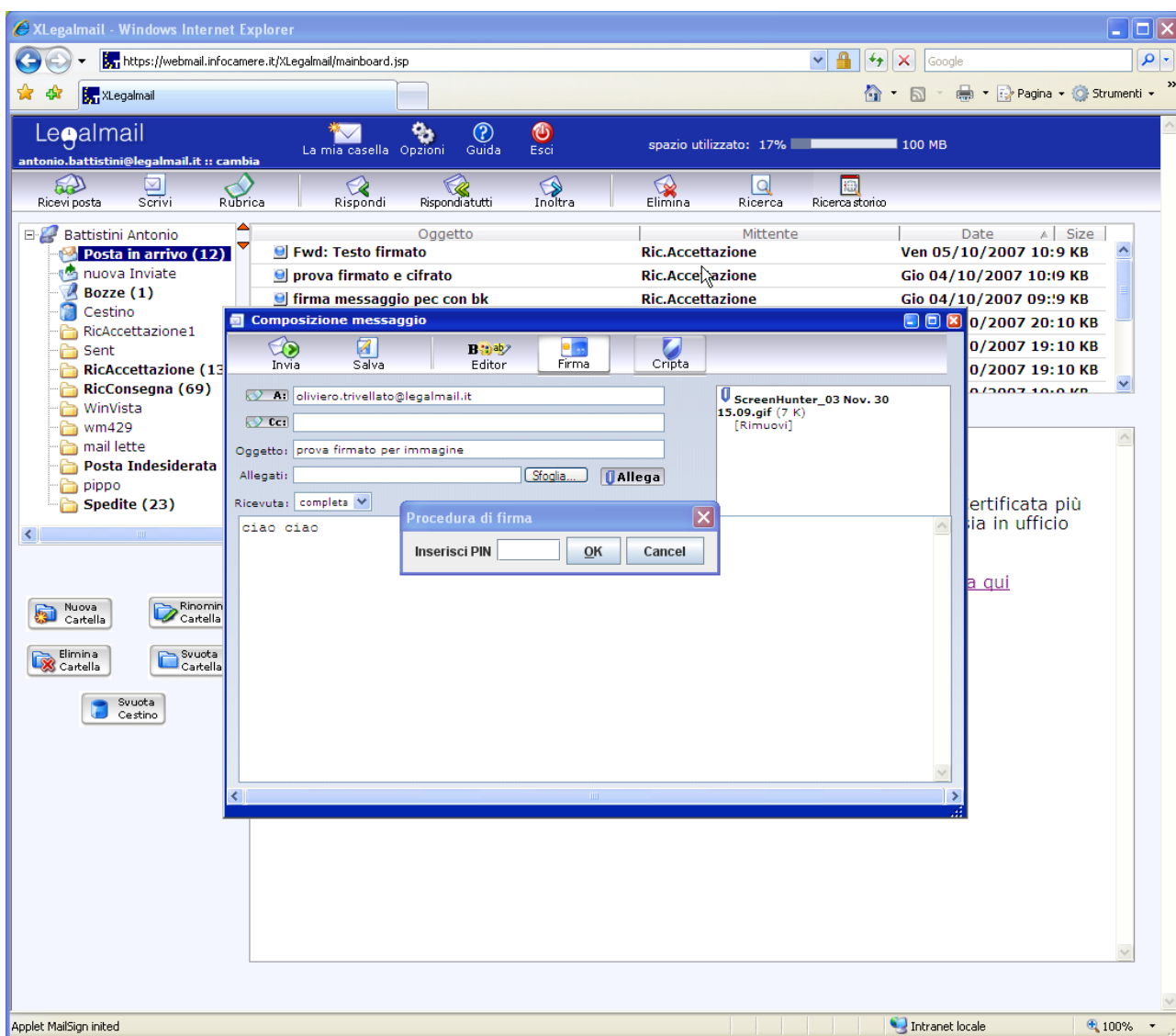
Si possono selezionare le seguenti tre modalità:

- **Firmato:** il messaggio inviato è un messaggio di posta certificata (quindi firmato dal provider) e firmato digitalmente dall'utente attraverso la propria SmartCard rilasciata da InfoCert utilizzando la chiave privata del proprio certificato di autenticazione
- **Criptato:** il messaggio inviato è un messaggio di posta certificata (quindi firmato dal provider) e criptato per garantire maggiore riservatezza, usando la chiave pubblica del certificato di autenticazione del destinatario

- **Firmato e Criptato:** il messaggio inviato è un messaggio di posta certificata (quindi firmato dal provider), firmato digitalmente dall'utente attraverso la propria SmartCard rilasciata da InfoCert e 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 avvisa con una finestra l'esito dell'invio.

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**.

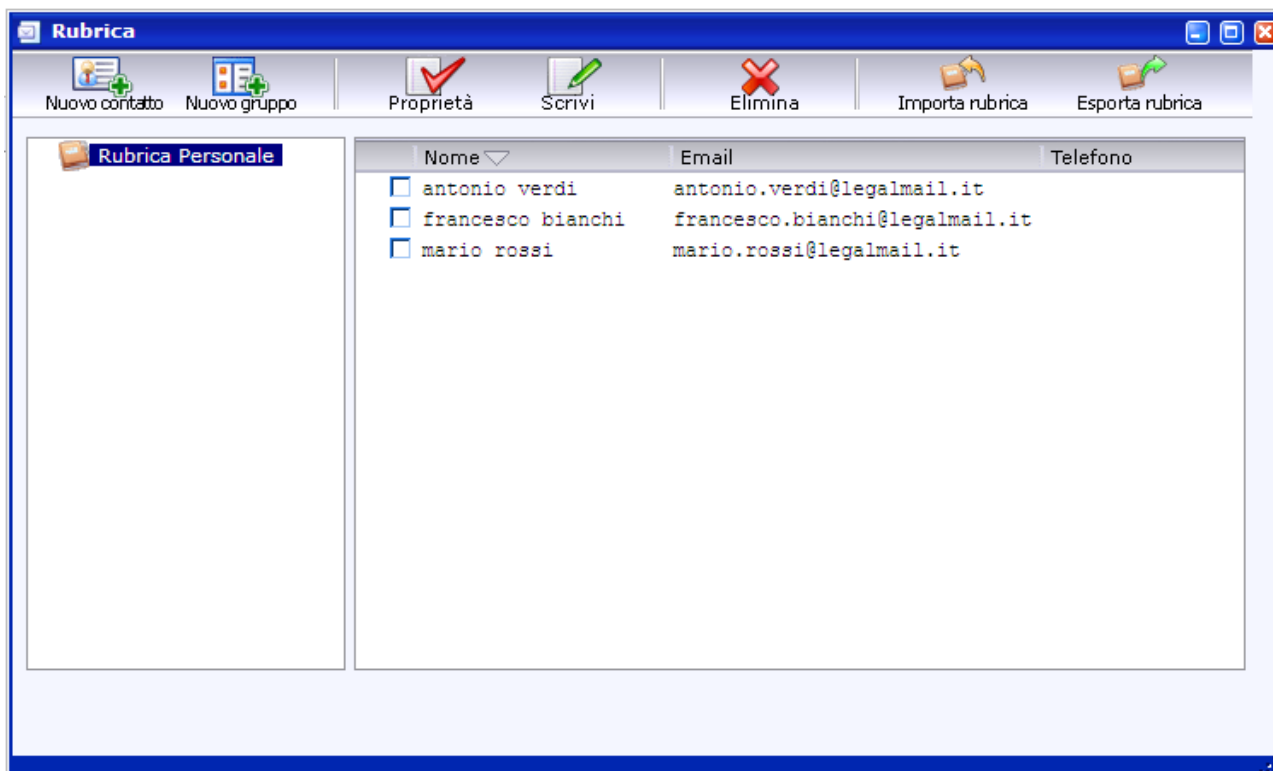


N.B. Se l'utente vuole crittografare il messaggio è necessario che mittente e destinatario abbiano un certificato conosciuto da webmail. Se il mittente non ha il certificato del destinatario l'invio viene effettuato, ma il mittente non potrà più leggere il messaggio inviato. Per conoscere il certificato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

15. Rubrica






Ogni utente può crearsi la rubrica personale degli indirizzi di posta. Inoltre è possibile archiviare i certificati digitali.



La maschera della rubrica permette di inserire, modificare, cancellare un indirizzo di posta all'interno della propria rubrica; inoltre è possibile creare e gestire gruppi di indirizzi di posta.



Nella parte destra della maschera l'utente trova l'elenco degli indirizzi inseriti nella rubrica. I tasti consentono di modificare o cancellare l'indirizzo di posta selezionato (flag a sinistra dell'indirizzo). La parte sinistra permette la navigazione all'interno dei gruppi creati dall'utente.

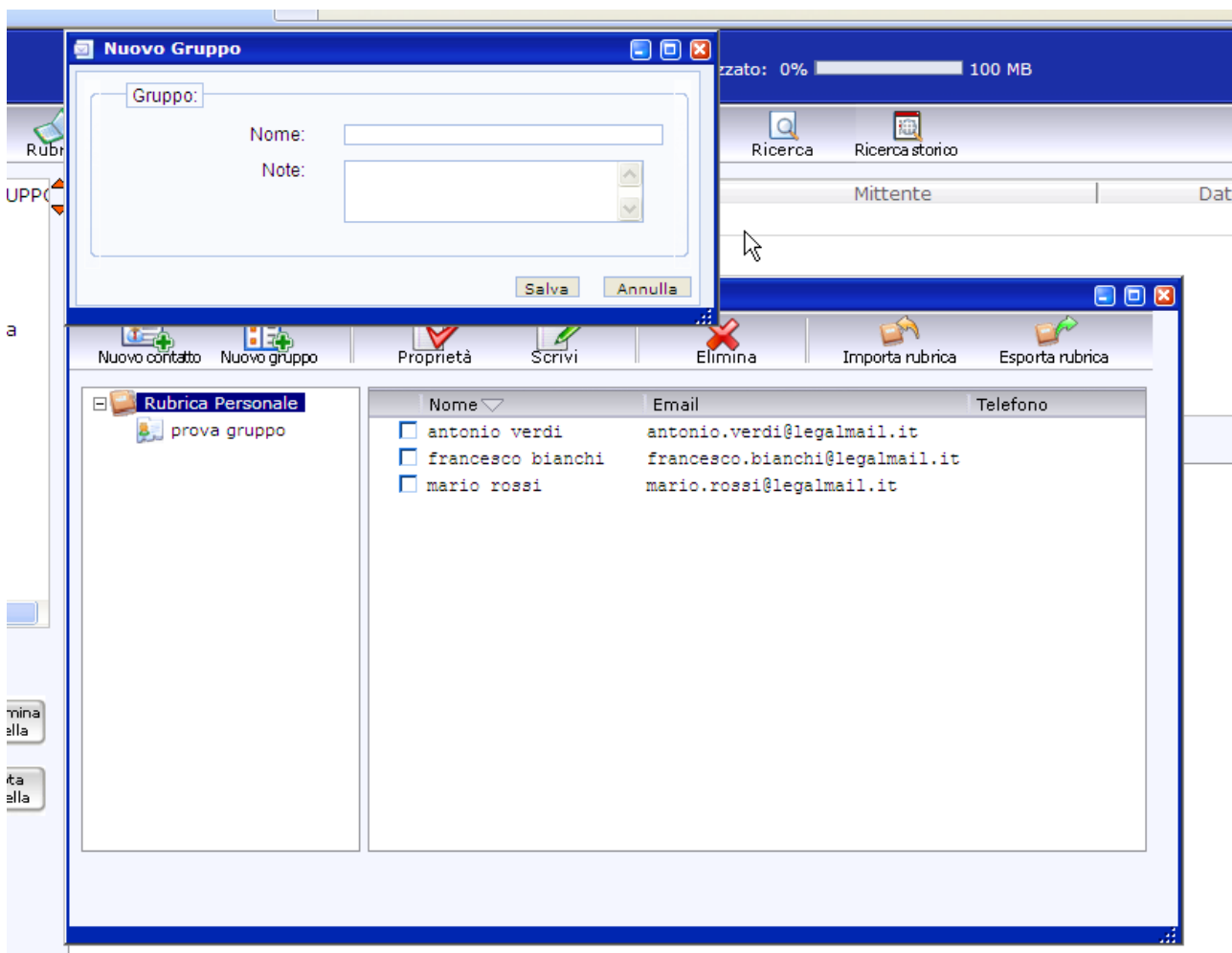
Descrizione della barra dei strumenti:

	Aprire la finestra di inserimento nuovo contatto
	Aprire la finestra di inserimento di un nuovo gruppo
	Aprire la finestra
	Una volta selezionati i destinatari, questo bottone permette di aprire la finestra di composizione del messaggio con i destinatari già impostati
	Elimina il/i contatti/gruppi selezionati

 Importa rubrica	Permette di importare in rubrica dei contatti a partire da un file (p.e. Un file di indirizzi creato con Outlook)
 Esporta rubrica	Permette di esportare in un file i contatti presenti in rubrica

15.1 Inserire un gruppo in rubrica:

Per inserire un nuovo gruppo in rubrica cliccare sul bottone “Nuovo Gruppo” appare la finestra sottostante:

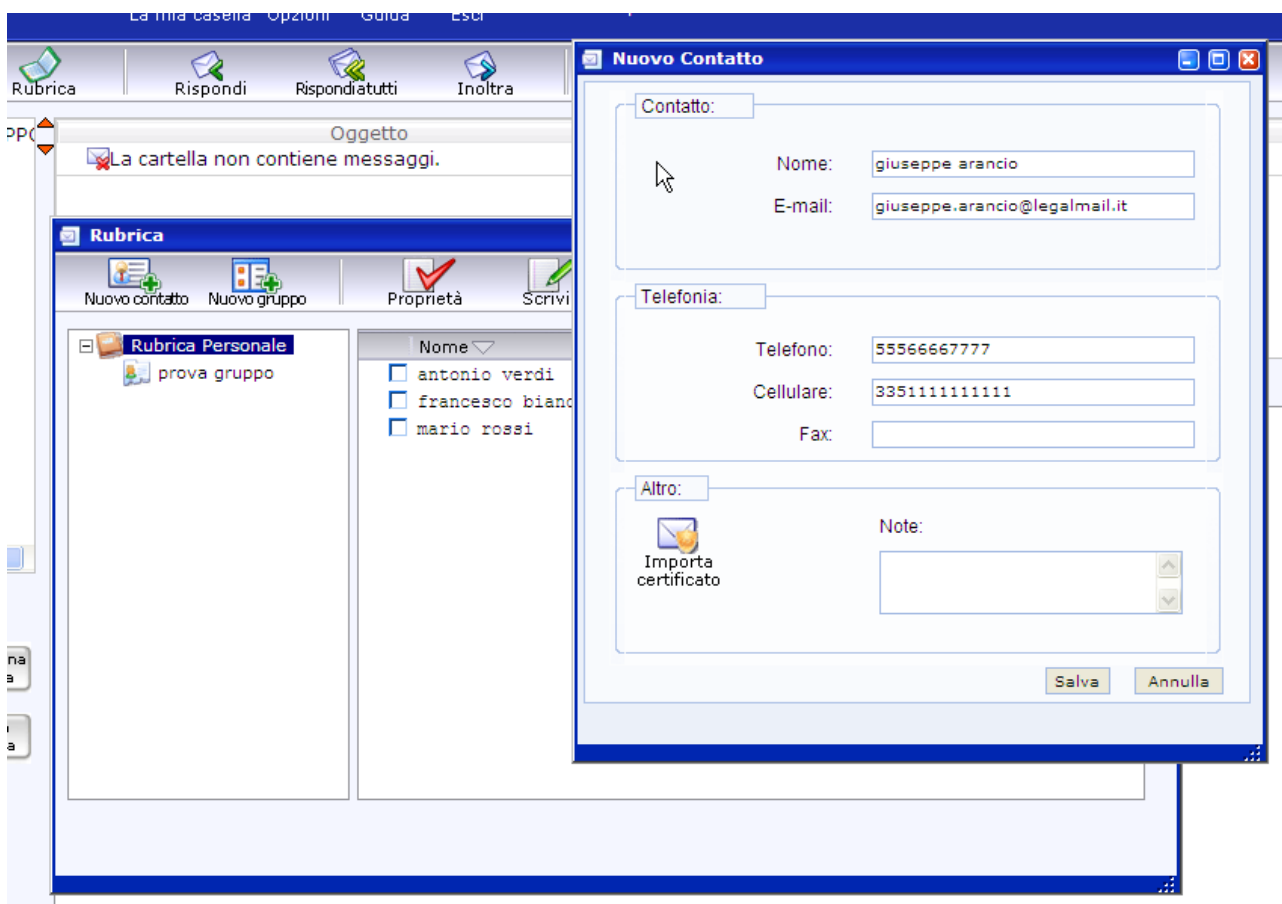


inserire il nome del gruppo desiderato nel campo “Nome” ed eventualmente aggiungere delle note. Premere il bottone “Salva” per salvare il gruppo.

Per associare uno o più indirizzi al gruppo, posizionarsi in Rubrica personale, selezionare il contatto, con il trasto sinistro del mouse premuto, trascinare il contatto sopra il gruppo desiderato e rilasciare il tasto del mouse. Ripetere l'operazione per ogni contatto da aggiungere al gruppo. Se un contatto è già presente all'interno del gruppo apparirà una finestra di errore per contatto già presente.

15.2 Inserire un contatto in rubrica:

Per inserire un contatto in rubrica posizionarsi col mouse sulla Rubrica personale (evidenziata come in figura), cliccare il bottone “Nuovo contatto” e si aprirà la finestra “Nuovo Contatto”:



compilare i campi **Nome** ed **E-Mail**. E' possibile associare anche altre informazioni quali i recapiti telefonici e delle note relative al contatto.

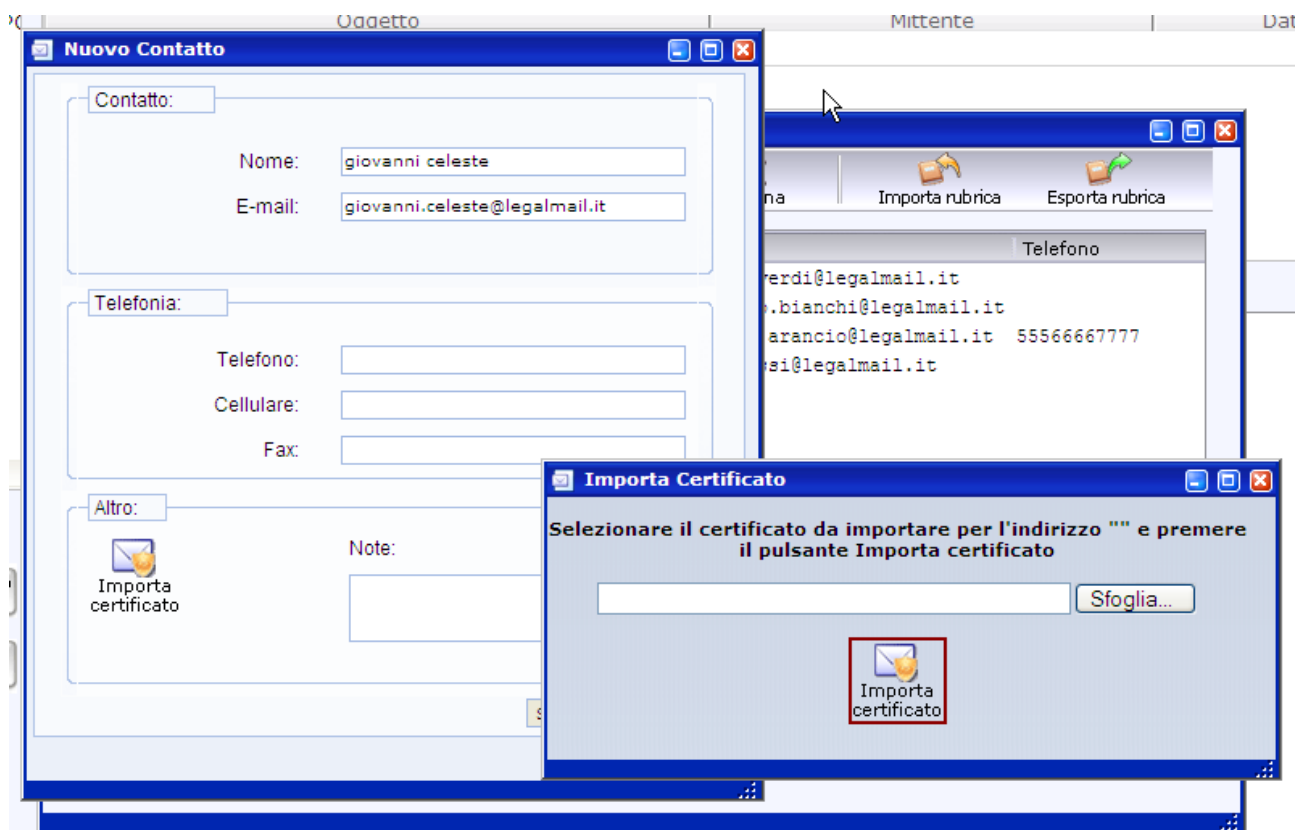
Una volta inserite le informazioni premere il bottone “Salva”; se l'operazione avrà esito positivo apparirà il messaggio “Contatto aggiunto con successo”

Se si possiede il certificato digitale del contatto, tramite il bottone “Importa certificato” è possibile associare al contatto il suo certificato.

Si apre una nuova finestra Importa certificato (come appare in figura) e cliccando il bottone sfoglia è possibile selezionare dal proprio computer il file del certificato da importare. Una volta selezionato premere il bottone “Importa Certificato”

Questo permetterà in seguito di decifrare i messaggi cifrati provenienti da quel mittente.

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

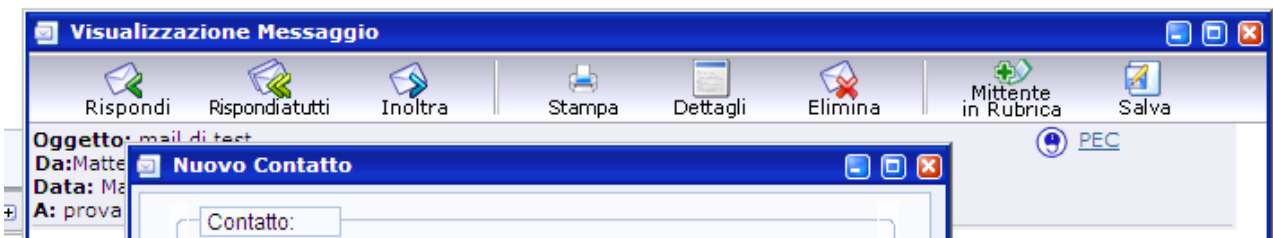


l'intestazione del nome in rubrica sembri corretta, l'indirizzo inserito in rubrica non risulterà corretto: verrà inserito l'indirizzo del provider del mittente e i messaggi spediti non arriveranno mai alla giusta destinazione.

In fase di composizione del messaggio per inserire l'indirizzo e-mail nell'apposito campo è possibile o digitare l'indirizzo, o reperirlo dalla rubrica cliccando sul bottone "A:" anche i destinatari per copia conoscenza (CC:) possono essere reperiti dalla rubrica personale cliccando l'apposito bottone a sinistra del campo.

E' possibile in qualsiasi momento modificare o importare il certificato di un contatto cliccando il bottone "Proprietà" appare la finestra "Modifica Contatto"

E' inoltre possibile aggiungere un contatto in Rubrica personale partendo dalla finestra "Visualizzazione messaggio" cliccando il bottone "Mittente in rubrica"



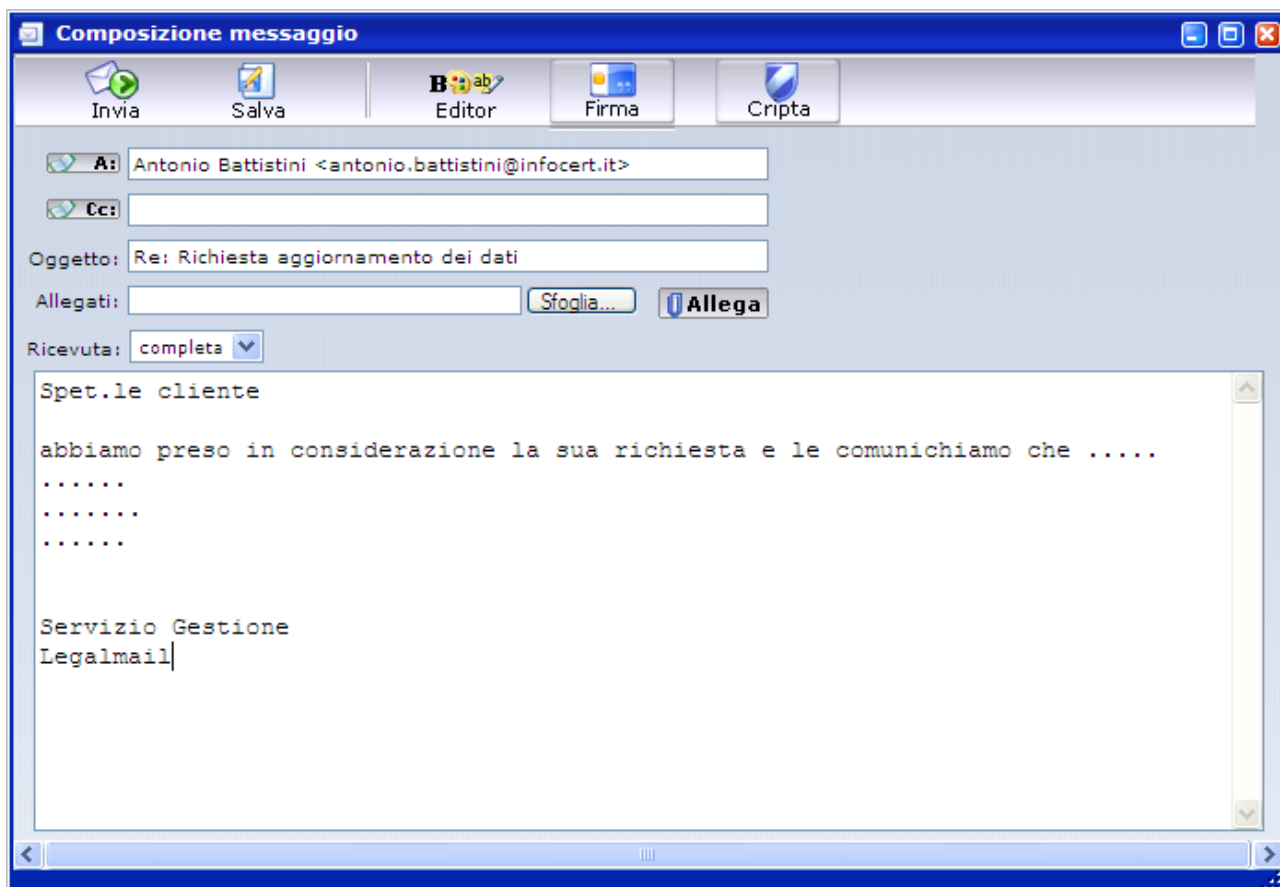
16. “Rispondi”, “Rispondi a tutti” e “Inoltra”

Questi bottoni permettono di rispondere rispettivamente:

- bottone “Rispondi”: permette di aprire la finestra di composizione nuovo messaggio con il destinatario/i già precompilato preso dal messaggio in arrivo selezionato in quel momento
- bottone “Rispondi a tutti”: permette di aprire la finestra di composizione messaggio con i campi del/dei destinatari presenti nel messaggio selezionato in quel momento e i destinatari presenti in copia conoscenza (CC:)
- bottone “Inoltra”: permette di inoltrare il messaggio selezionato a uno o più nuovi destinatari.

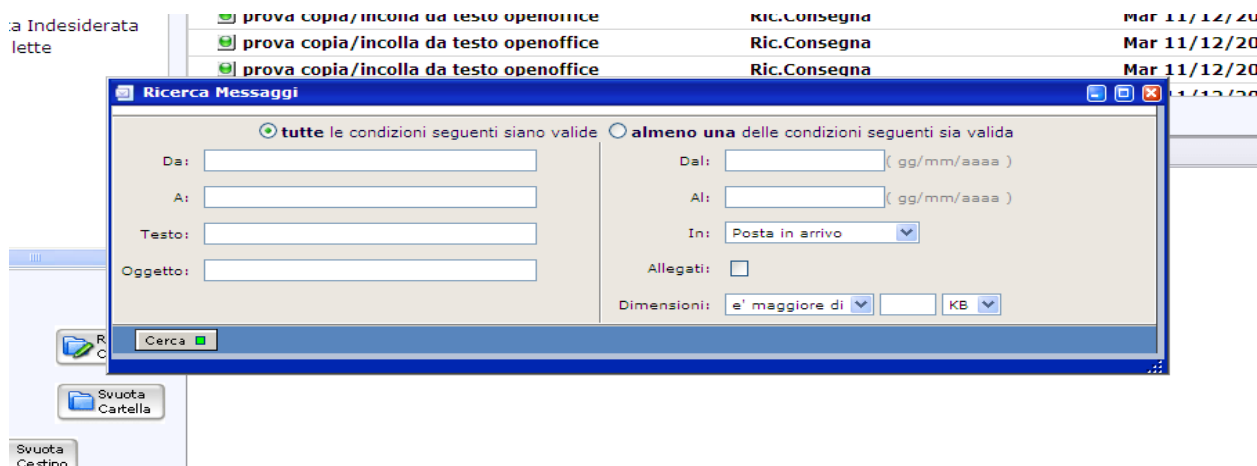
Nel caso di Risposta il nuovo messaggio avrà per oggetto lo stesso del messaggio selezionato preceduto dalla sigla “Re:” e conterrà il testo del messaggio originale a cui si sta rispondendo se sulla scheda “Opzioni” è stato selezionato il flag “*Includi il testo originale del messaggio nella risposta e per indicare il testo originale usa il carattere:*”

Nel caso di Inoltra il nuovo messaggio avrà per oggetto lo stesso del messaggio selezionato, preceduto dalla sigla “Fwd:”. Il messaggio originale sarà invece inserito come allegato al presente messaggio.



17. Ricerca

Per cercare i messaggi all'interno della propria casella è possibile utilizzare il bottone “Ricerca” che tramite una finestra opportuna permette di eseguire delle ricerche secondo parametri selezionabili dall'utente. Di seguito la finestra di ricerca:

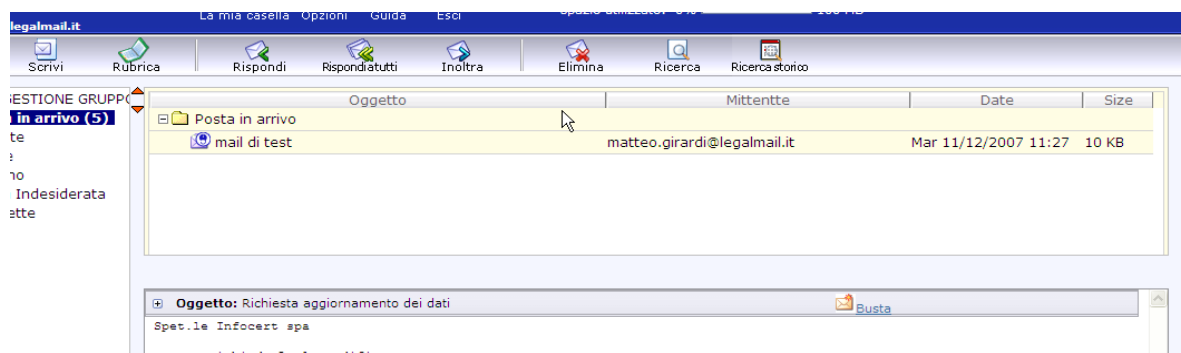


è possibile eseguire ricerche inserendo una o più condizioni che dovranno essere verificate dal sistema.

Si possono effettuare ricerche per:

- mittente
- destinatario
- parole sul testo del messaggio
- parole sull'oggetto del messaggio
- intervalli di data dal: xxxxxx al: xxxxx
- in cartelle specifiche o in tutte le cartelle
- comprendere gli allegati nel testo da ricercare
- ricercare per dimensione del messaggio

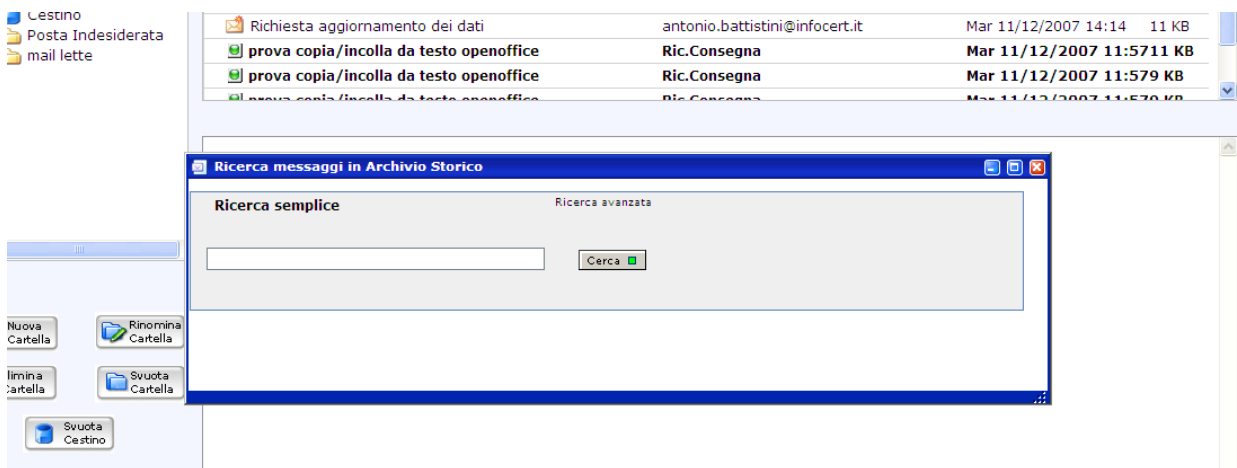
Se esistono dei messaggi che soddisfano alla ricerca, questi saranno visualizzati all'interno dell'area “Lista dei messaggi”

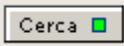


N.B. La “Lista dei messaggi” ha un colore giallo che sta ad indicare che ci si trova all'interno di una selezione dovuta ad una ricerca.

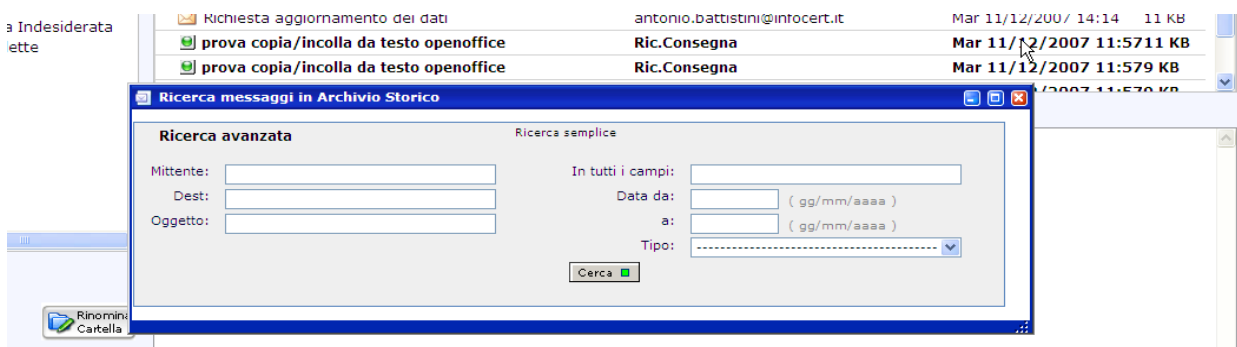
18. Ricerca Storico


Per cercare i messaggi salvati in “archivio storico”, Cliccare sul bottone “Ricerca Storico”. Si accede in questo modo alla finestra “Ricerca messaggi in Archivio Storico” nella modalità di ricerca semplice:



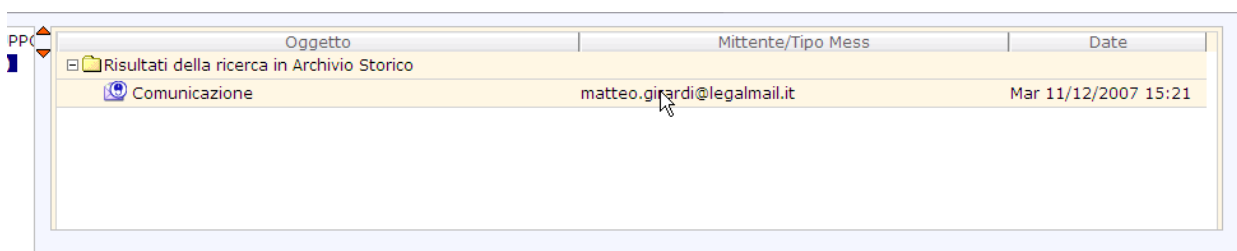
In questa finestra è possibile ricercare tra i messaggi archiviati attraverso un testo libero, come con un normale motore di ricerca: digitando un testo e selezionando il pulsante  è possibile visualizzare l'elenco dei messaggi contenenti quel testo.

Selezionando [Ricerca avanzata](#) si accede alla seguente finestra:



In questa finestra è possibile fare delle ricerche più puntuali, impostando i singoli campi normalmente utilizzati nella posta elettronica: mittente, destinatari, oggetto, testo contenuto, data di spedizione e tipo di messaggio. Cliccando sul pulsante , il sistema individuerà i messaggi che soddisfano tutte condizioni di ricerca impostate.

Anche in questo caso il risultato sarà evidenziato nella sezione “Lista dei messaggi”



19. Segnalazioni di esaurimento dello spazio a disposizione

Qualora lo spazio a disposizione per il salvataggio sia in esaurimento, il sistema www.Legalmail.it invia automaticamente dei messaggi alla casella di Posta Certificata dell'utente interessato. In particolare viene inviato un messaggio ogni qual volta che:

- lo spazio occupato supera il 75% dello spazio totale a disposizione;
- un messaggio non viene archiviato per mancanza di spazio sufficiente.

I messaggi di segnalazione non vengono in alcun caso salvati nell'archivio, pertanto non occuperanno ulteriore spazio, né potranno generare ulteriori segnalazioni.

20. 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: il contenuto e il significato sono gli stessi varia la forma grafica.

Nota:

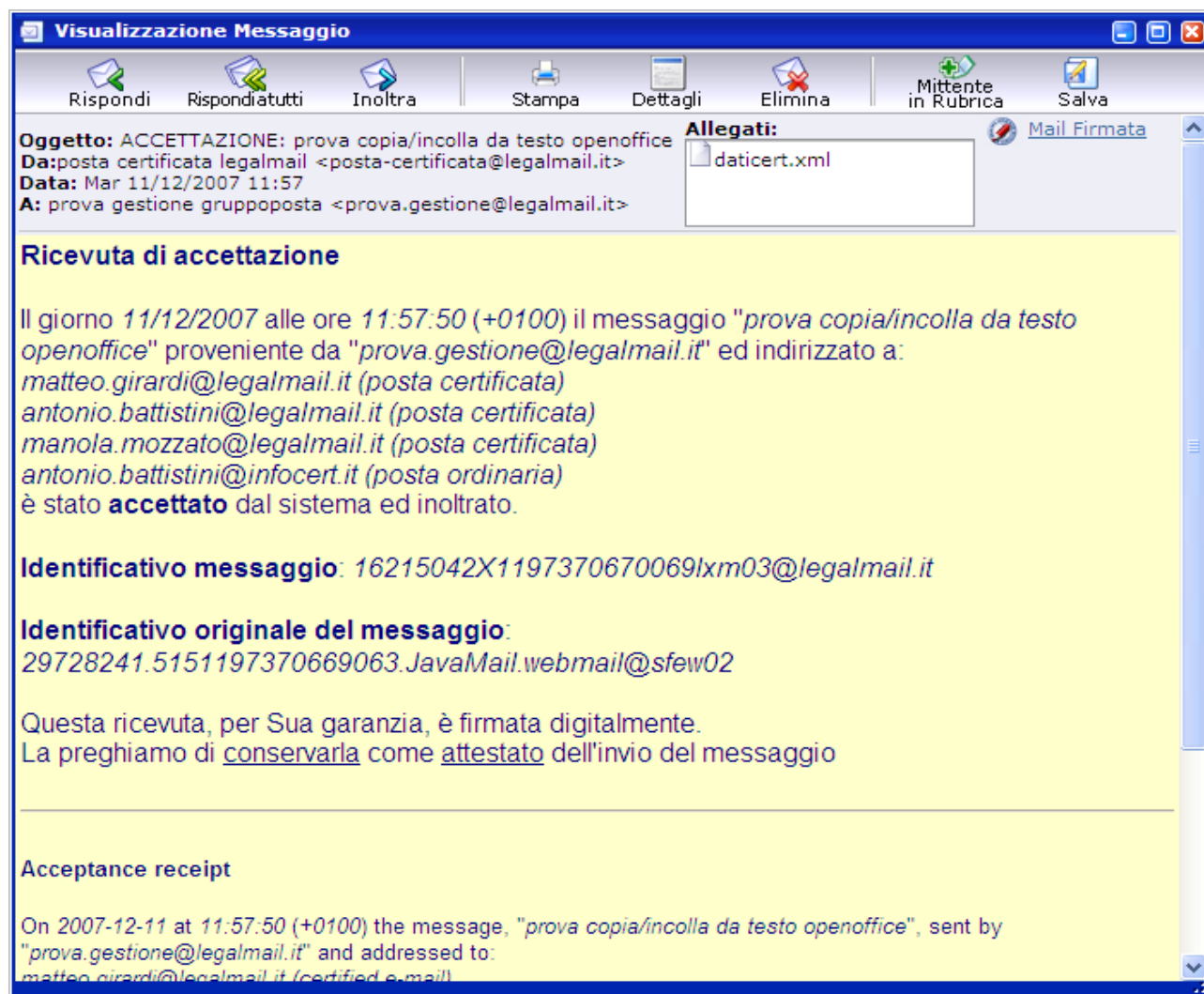
alcuni client di posta aprono in automatico certe tipologie di allegati; per questo motivo l'utente potrà non trovare alcuni degli allegati descritti nei paragrafi successivi. Per esempio alcuni client aprono automaticamente l'allegato postacert.eml: il testo dell'allegato viene "attaccato" di seguito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

20.1.1 Ricevuta di Accettazione

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

- Dati del messaggio e allegati
- Ricevuta di accettazione



The screenshot shows a webmail interface with a toolbar at the top containing icons for 'Rispondi', 'Rispondiatutti', 'Inoltra', 'Stampa', 'Dettagli', 'Elimina', 'Mittente in Rubrica', and 'Salva'. The message header includes:

Oggetto: ACCETTAZIONE: prova copia/incolla da testo openoffice
Da: posta certificata legalmail <posta-certificata@legalmail.it>
Data: Mar 11/12/2007 11:57
A: prova gestione gruppoposta <prova.gestione@legalmail.it>

Allegati: daticert.xml

Ricevuta di accettazione

Il giorno 11/12/2007 alle ore 11:57:50 (+0100) il messaggio "prova copia/incolla da testo openoffice" proveniente da "prova.gestione@legalmail.it" ed indirizzato a:
 matteo.girardi@legalmail.it (posta certificata)
 antonio.battistini@legalmail.it (posta certificata)
 manola.mozzato@legalmail.it (posta certificata)
 antonio.battistini@infocert.it (posta ordinaria)
 è stato **accettato** dal sistema ed inoltrato.

Identificativo messaggio: 16215042X1197370670069lxm03@legalmail.it

Identificativo originale del messaggio:
 29728241.5151197370669063.JavaMail.webmail@sfew02

Questa ricevuta, per Sua garanzia, è firmata digitalmente.
 La preghiamo di conservarla come attestato dell'invio del messaggio

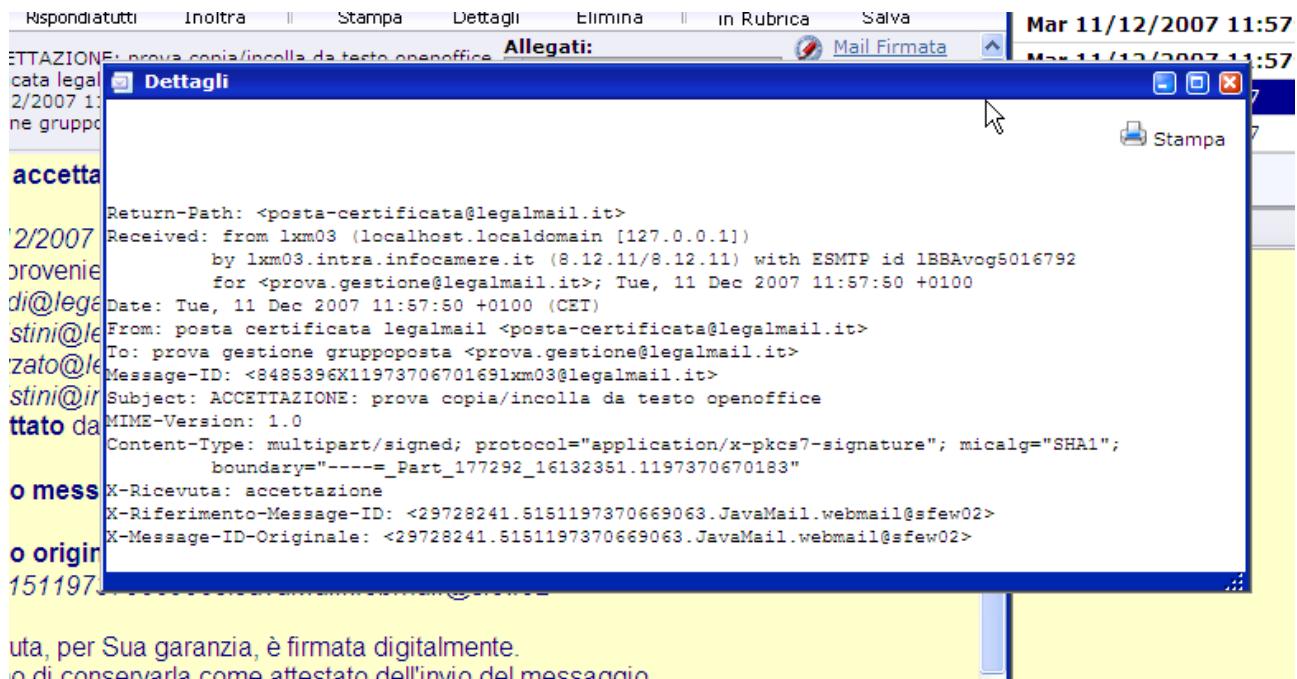
Acceptance receipt

On 2007-12-11 at 11:57:50 (+0100) the message, "prova copia/incolla da testo openoffice", sent by "prova.gestione@legalmail.it" and addressed to: matteo.girardi@legalmail.it (certified e-mail)

La prima parte contiene le informazioni del mittente, altri destinatari, oggetto, la possibilità di verificare la firma (bottone “Mail Firmata”) 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 datichert.xml contenente i dati di certificazione (vedi es. sotto)

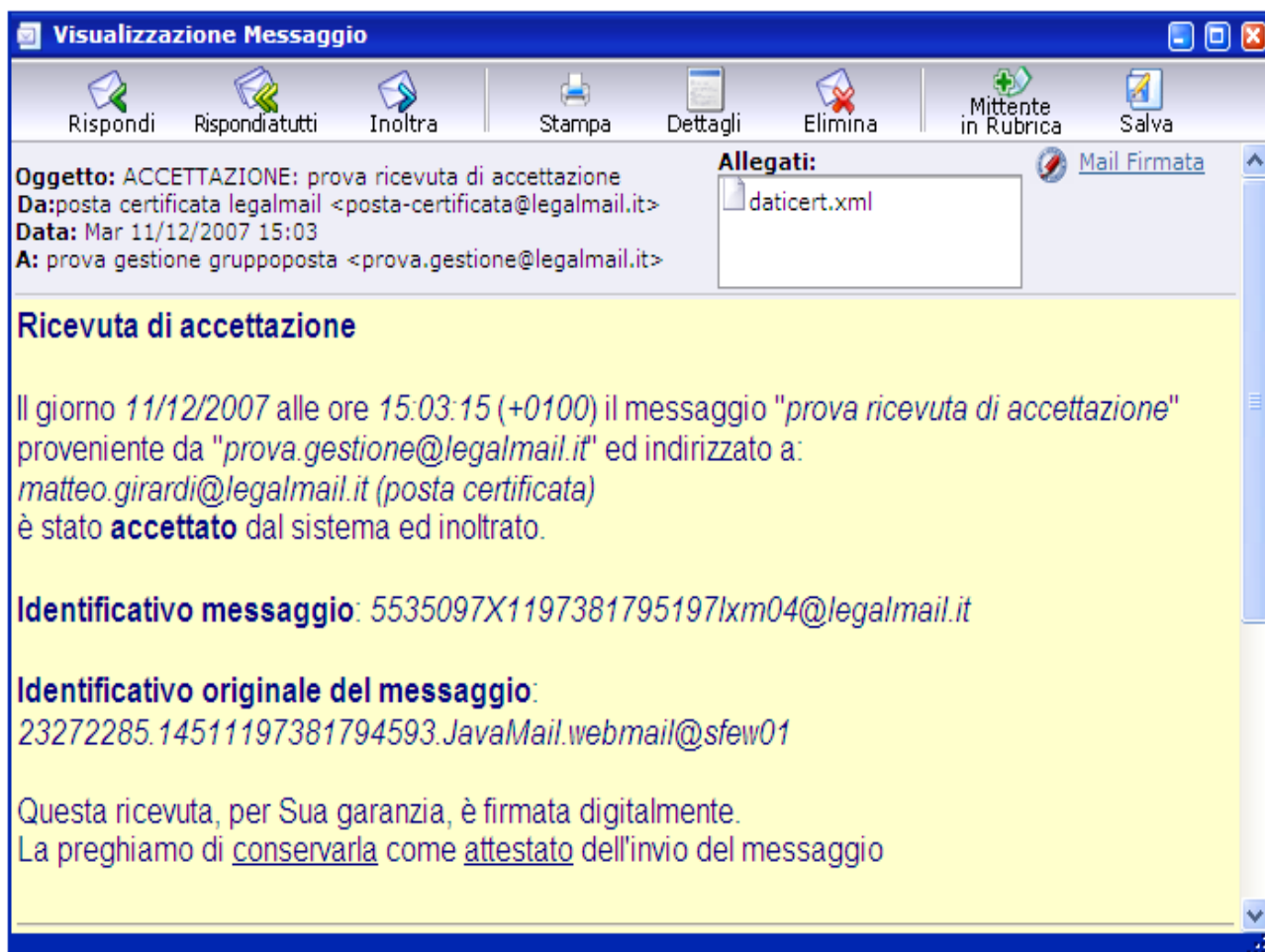
Il bottone “dettagli” presente sulla barra dei strumenti consente di accedere alle informazioni sulla spedizione del messaggio



MU/PEC – Legalmail Posta Certificata Manuale utente - Ver. 1 del 15/01/2008

pag. 57 di 66

La parte (Ricevuta di accettazione) riporta informazioni dettagliate sul messaggio (data e ora di invio, mittente, destinatario ecc..) inoltre contiene alcune informazioni sulla posta certificata e sul significato/valore delle ricevute come è possibile vedere nella seguente maschera:



Visualizzazione Messaggio

Rispondi Rispondiatutti Inoltra Stampa Dettagli Elimina Mittente in Rubrica Salva

Oggetto: ACCETTAZIONE: prova ricevuta di accettazione
Da: posta certificata legalmail <posta-certificata@legalmail.it>
Data: Mar 11/12/2007 15:03
A: prova gestione gruppoposta <prova.gestione@legalmail.it>

Allegati:
 daticert.xml

Ricevuta di accettazione

Il giorno 11/12/2007 alle ore 15:03:15 (+0100) il messaggio "prova ricevuta di accettazione" proveniente da "prova.gestione@legalmail.it" ed indirizzato a: matteo.girardi@legalmail.it (posta certificata) è stato **accettato** dal sistema ed inoltrato.

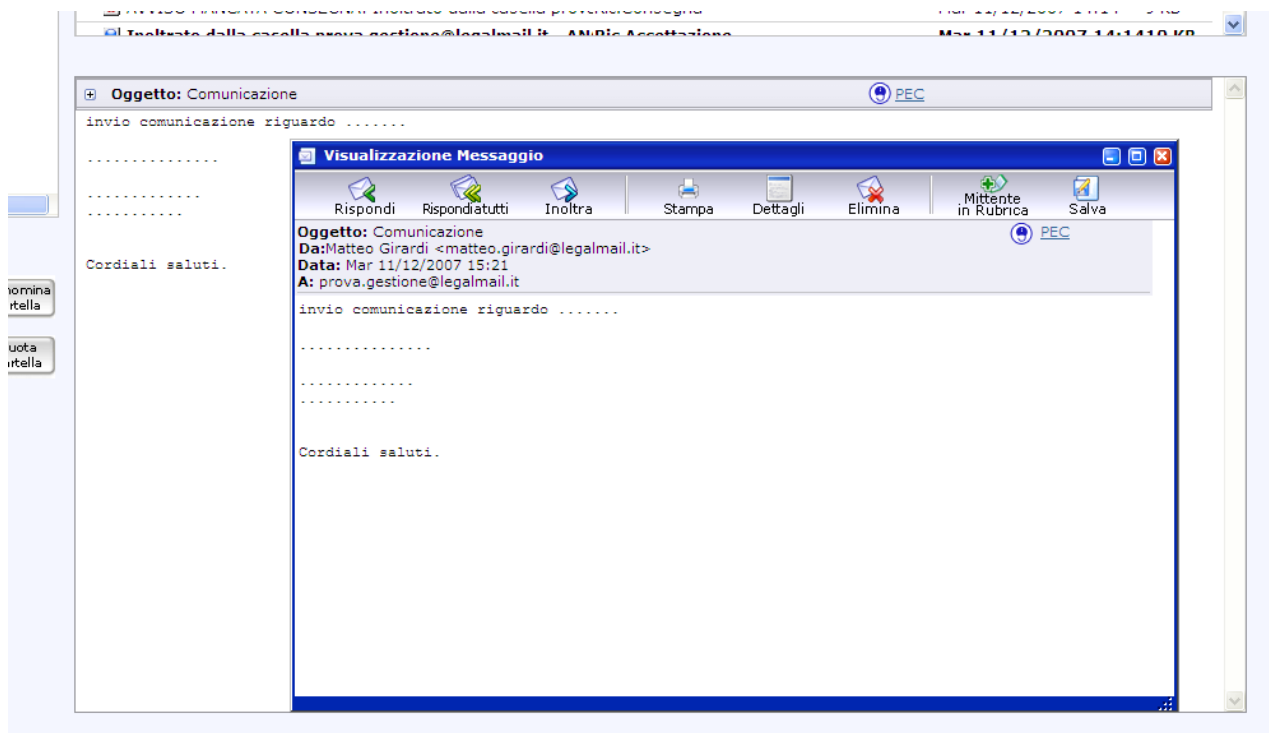
Identificativo messaggio: 5535097X1197381795197lxm04@legalmail.it

Identificativo originale del messaggio:
 23272285.14511197381794593.JavaMail.webmail@sfew01

Questa ricevuta, per Sua garanzia, è firmata digitalmente.
 La preghiamo di conservarla come attestato dell'invio del messaggio

20.1.2 Messaggio di Posta Certificata

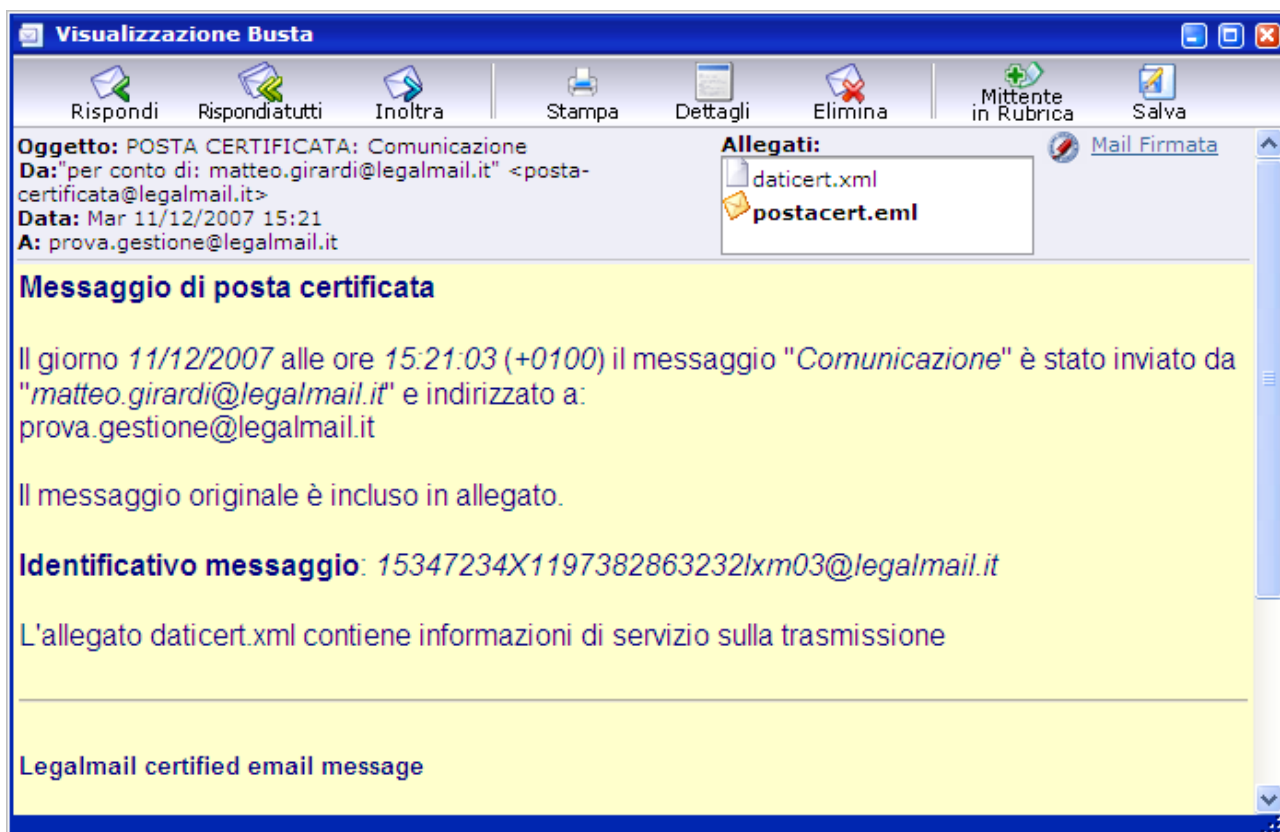
E' il messaggio che l'utente destinatario riceve da un altro utente con casella di posta certificata: appare subito il messaggio originale e solo a richiesta viene visualizzata la busta (messaggio di trasporto). Per i messaggi crittografati consultare l'apposito paragrafo.



Premendo il bottone  è possibile aprire la finestra “Visualizzazione busta”, questa contiene:

- 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)
- Estremi del messaggio (contiene le informazioni su data e ora di spedizione, mittente e identificativo del messaggio)

Di seguito la finestra “Visualizzazione Busta”



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](#))

20.1.3 Ricevuta di Consegna

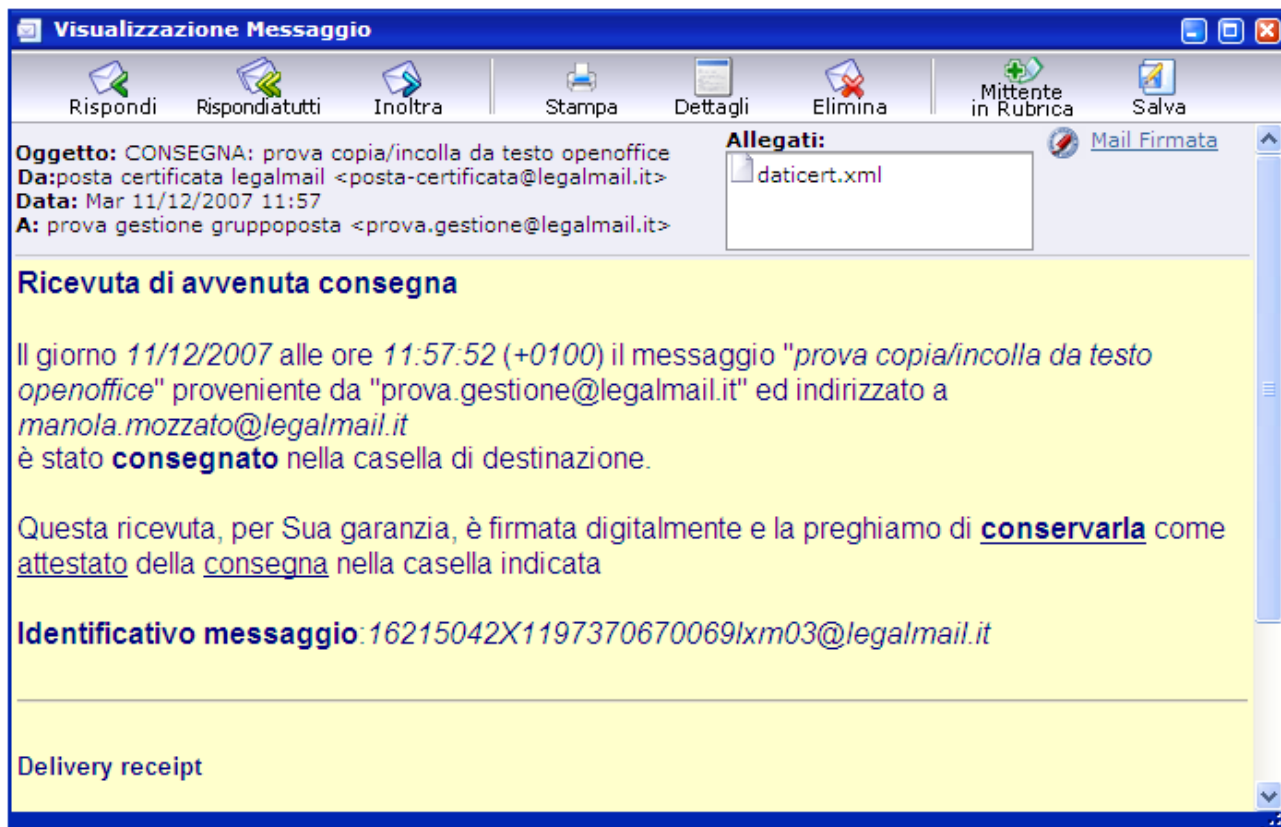
E' il messaggio inviato dal gestore di posta certificata del destinatario. Contiene le informazioni che certificano l'avvenuta consegna del messaggio nella casella di posta certificata del destinatario. La ricevuta di consegna ha in allegato il messaggio originale inviato dal mittente ai soli destinatari diretti (TO) a meno di disposizioni contrarie da parte del mittente.

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)

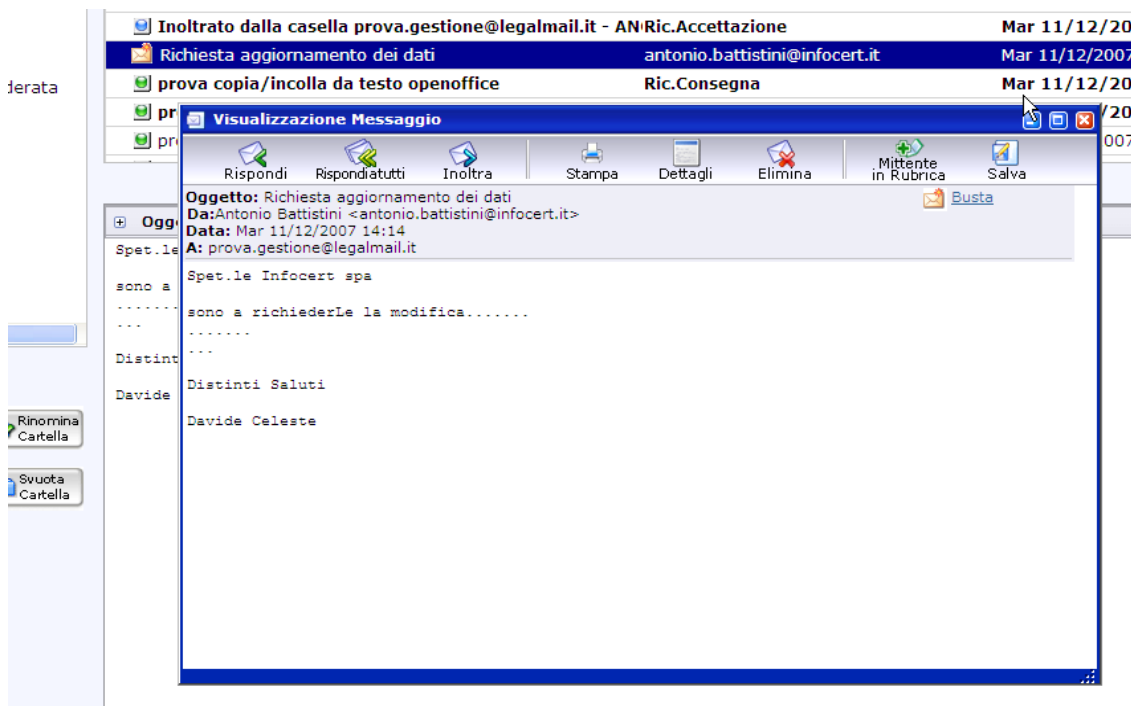
Se il messaggio è stato crittografato occorre utilizzare la modalità avanzata: se l'utente sta utilizzando la modalità normale un messaggio lo avvisa (cfr. [Ricezione di messaggi crittografati](#))



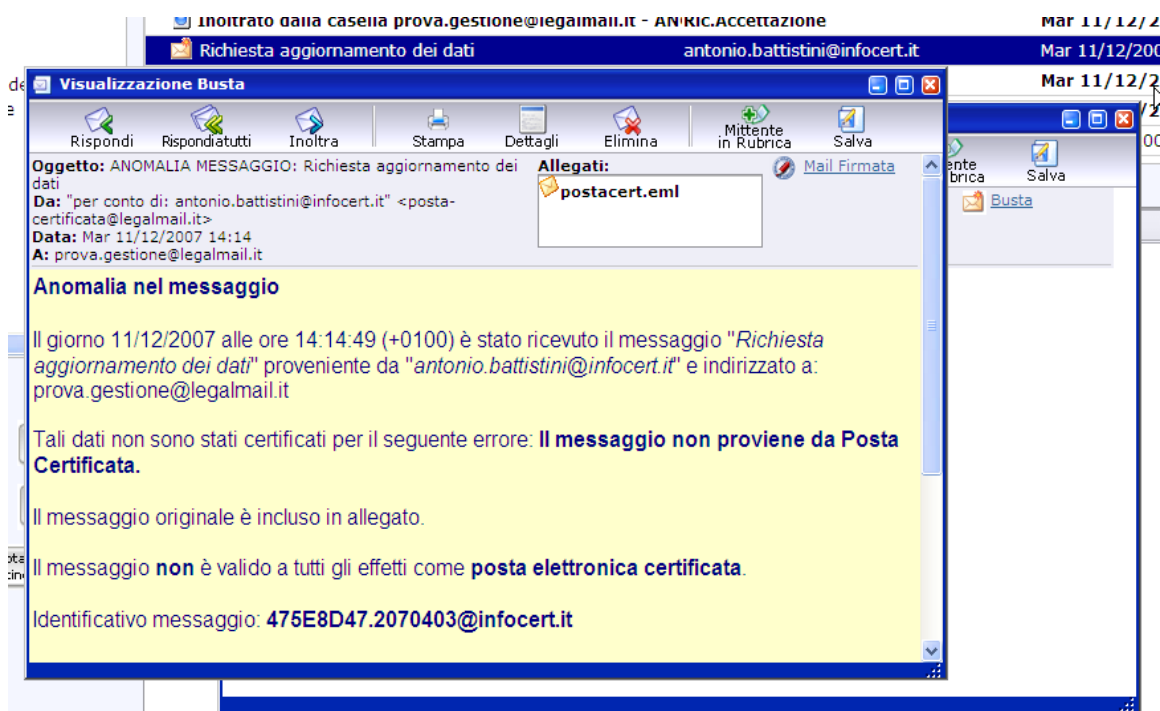
20.1.4 Messaggio da posta ordinaria:

Nel caso l'utente riceva un messaggio da una casella non di posta certificata il sistema identifica il messaggio e lo inserisce nella busta "Anomala di messaggio" per isolarlo e indicare che il messaggio non proviene da Posta Certificata come è possibile vedere dalla maschera seguente: di seguito viene riportato un esempio di messaggio da posta non certificata e la relativa "Busta di Anomalia"

- Messaggio proveniente da posta ordinaria (non certificata) Evidenziato anche dalla busta presente sulla destra della finestra



- Busta di Anomalia



21. Malfunzioni connesse alla firma elettronica

I problemi connessi con i certificati utilizzati per firmare i messaggi di posta elettronica certificata possono essere di varia natura; i principali sono:

1. il messaggio è stato alterato: **problema molto grave, la trasmissione non è valida**. In posta certificata non deve mai capitare, se capita il problema va segnalato.
2. non è stato specificato se accettare il certificato; **capita normalmente**: di seguito sono fornite le istruzioni su come comportarsi.
3. il certificato di firma è scaduto; capita normalmente: di seguito sono fornite le istruzioni su come comportarsi
4. il certificato non contiene l'indirizzo di posta elettronica del mittente; in posta certificata non dovrebbe mai capitare
5. è impossibile determinare se il certificato sia stato revocato o no; in posta certificata questo non rappresenta un problema

22. Termini e definizioni

22.1 Riferimenti normativi e tecnici

Riferimenti normativi

1. Decreto del Presidente della Repubblica 7 Aprile 2003, n.137 (G.U. n.138 del 17 Giugno 2003)
2. Decreto legislativo 7 marzo 2005, n. 82 (in G.U. n. 112 del 16 maggio 2005 - S.O. n. 93) - Codice dell'amministrazione digitale (nel seguito referenziato come CAD)
3. Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001) e sue modificazioni secondo DPR 137/2003 (nel seguito referenziato come TU)
4. Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 (G. U. n. 98 del 27/04/2004)
5. Decreto Ministeriale del 2 novembre 2005 recante “Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata” (GU n.266 del 15/11/2005)
6. Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.

Riferimenti tecnici

- RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)
- RFC 1891 (SMTP Service Extension for Delivery Status Notifications)
- RFC 1912 (Common DNS Operational and Configuration Errors)
- RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions)
- RFC 2315 (PKCS #7: Cryptographic Message Syntax Version 1.5)
- RFC 2633 (S/MIME Version 3 Message Specification)
- RFC 2660 (The Secure HyperText Transfer Protocol)
- RFC 2821 (Simple Mail Transfer Protocol)
- RFC 2822 (Internet Message Format)
- RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification)
- RFC 3174 (US Secure Hash Algorithm 1 – SHA1)
- RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security)
- RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile)
- Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8

22.2 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti nelle norme sopra referenziate si rimanda alle definizioni in essi stabilite. Dove appropriato viene indicato tra parentesi graffe il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Allegato/i:

i documenti tecnici che descrivono in maniera analitica il Servizio di posta elettronica certificata Legalmail e le condizioni per la prestazione degli stessi che costituiscono parte integrale e sostanziale del Contratto;

Autorità per la marcatura temporale {Time-stamping authority}

È il sistema software/hardware, gestito da un Certificatore accreditato, che eroga il servizio di marcatura temporale.

Avviso di mancata consegna – [5]

Avviso di non accettazione – [5]

Busta di anomalia – [5]

Busta di trasporto – [5]

Casella di posta elettronica certificata – [5]

Dati di certificazione – [5]

Destinatario – [8]

Dominio di posta elettronica certificata – [5]

Firma elettronica – [TU]

Firma elettronica qualificata – [TU]

Firma digitale {*digital signature*} – [TU]

CAD – Codice dell'amministrazione digitale

Ci si riferisce al Decreto legislativo 7 marzo 2005, n. 82 (in G.U. n. 112 del 16 maggio 2005 - S.O. n. 93)

Gestore/Provider di posta elettronica certificata – [5]

Indice dei gestori di posta elettronica certificata – [5]

Log dei messaggi – [8]

Marca temporale – [4]

Messaggio di posta elettronica certificata – [8]

Messaggio originale – [5]

Posta elettronica – [8]

Posta elettronica certificata – [8]

Punto di accesso – [5]

Punto di consegna – [5]

Punto di ricezione – [5]

Regole tecniche

Allegato al DM 2 novembre 2005 [5], recante le norme tecniche per il trattamento dei messaggi di Posta Elettronica Certificata.

Ricevuta breve di avvenuta consegna – [5]

Ricevuta completa di avvenuta consegna – [5]

Ricevuta di accettazione – [5]

Ricevuta di avvenuta consegna – [5]

Ricevuta di presa in carico – [5]

Ricevuta sintetica di avvenuta consegna – [5]

Riferimento temporale – [8]

Servizio Legalmail

è il servizio in base al quale InfoCert assegna al Cliente delle caselle di posta elettronica certificata a valore legale Legalmail conformi alle caratteristiche specificate nell'Allegato tecnico al DM [5].

Titolare – [5]

Utente di posta elettronica certificata – [8]

Virus informatico – [8]

Utilizzatore

soggetto a cui è assegnato dal Cliente l'utilizzo della casella di posta elettronica certificata Legalmail;

22.3 Acronimi e abbreviazioni

CNIPA – Centro Nazionale per l'informatica nella Pubblica Amministrazione

DPCM - Decreto del Presidente del Consiglio dei Ministri

Ci si riferisce al DPCM 13 gennaio 2004 recante “Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti”.

Indirizzo IP

Indirizzo numerico che identifica gli elaboratori connessi alla rete.

PEC – Posta Elettronica Certificata

PIN – Personal Identification Number

Codice associato ad una smart card, utilizzato dal Titolare per accedere alle funzioni della carta.

TU – Testo Unico

Ci si riferisce al DPR n. 445/2000 e sue successive modificazioni, , *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*.