

% 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 DM [5].

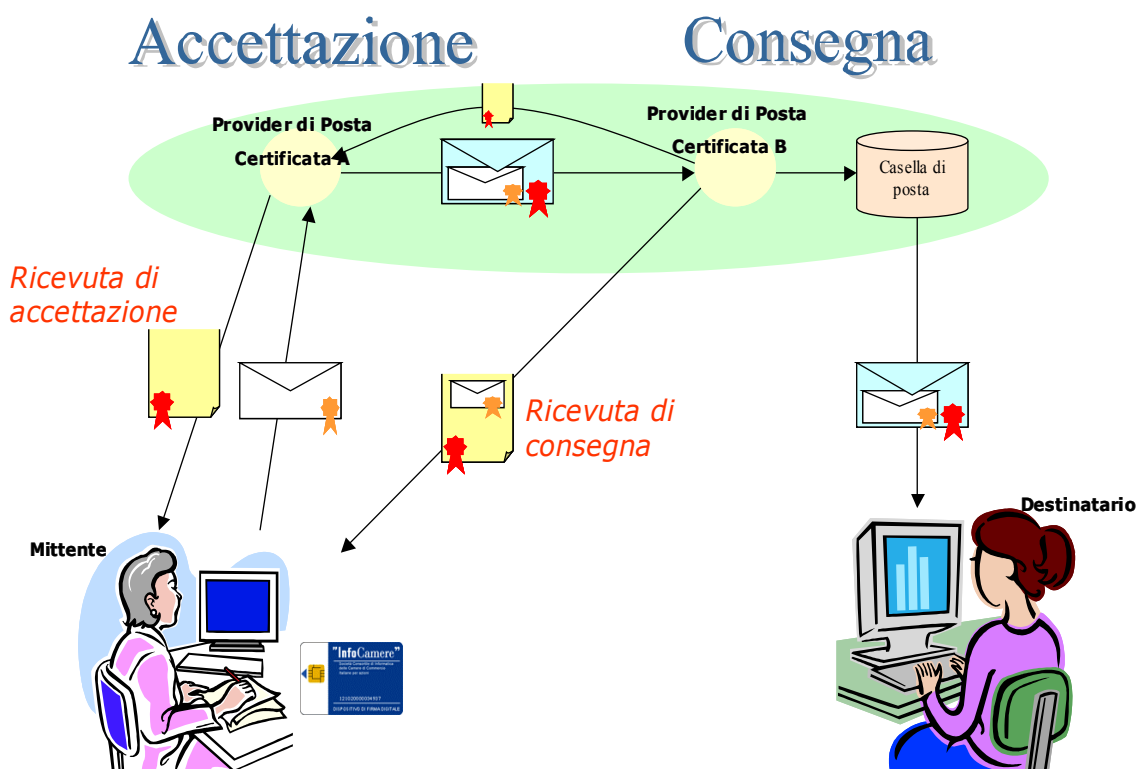


Figura 1

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.

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.

&" Validità legale

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 dalla normativa relativa alla Posta Elettronica Certificata.

Legalmail è pienamente conforme alle regole tecniche richiamate dal DM [5] e pubblicate dal CNIPA sul sito (www.cnipa.gov.it); le caratteristiche di queste caselle sono pertanto tali da renderle interoperabili con le caselle di posta elettronica certificata distribuite da altri gestori di posta certificata accreditati.

Nei casi consentiti dalla legge, la posta certificata può essere utilizzata in sostituzione della posta cartacea. I messaggi ricevuti nella casella di posta certificata si intendono **pervenuti** al titolare della casella.

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

' " Funzionalità standard

Le funzionalità più rilevanti 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 consegnata 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 dopo che l'utente ha scaricato e cancellato il messaggio dal server, a meno di disposizioni normative specifiche o di esplicita richiesta da parte del cliente (tramite adesione a servizi aggiuntivi).
- divieto di utilizzo dei destinatari nascosti (BCC o CCN)
- obbligo di almeno un destinatario in "TO (A)".
- 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.

4. 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:

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.

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 (errore formale, presenza di virus nel messaggio sottomesso dall'utente).

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.

3. le ricevute di preso in carico;

i sistemi di posta elettronica certificata del circuito notificano l'uno 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. 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)'.

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 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, viene meno l'opponibilità dello stesso.

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.

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

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.

Il Gestore controlla i messaggi di posta elettronica certificata in ingresso provenienti da altri gestori per verificare l'assenza di virus. I messaggi che contengono virus informatici non vengono inoltrati al destinatario e il Gestore 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.

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

Nel caso in cui il gestore destinatario non notifichi la "presa in carico" del messaggio entro 12 ore dalla sua spedizione, il mittente riceve, da parte del proprio gestore, un "avviso di mancata consegna per superamento dei tempi massimi previsti", ovvero una notifica che allerta sul possibile fallimento della consegna. Se il gestore destinatario non notifica la "consegna" entro le 24 ore successive alla spedizione, il mittente riceve, dal proprio gestore, un "avviso di mancata consegna".

) " Forzatura della password

In caso il titolare della casella abbia la necessità di forzare una nuova password per una casella PEC, deve seguire la seguente procedura:

- scaricare dal sito www.legalmail.it (sezione Documenti) il modulo apposito
- compilare il modulo e firmarlo
- inviare il modulo firmato via fax con allegato un documento di identità (o in alternativa firmato digitalmente via posta elettronica certificata):
 - all'intermediario di riferimento (per caselle attivate tramite intermediario)
 - all'Assistenza Legalmail (vedi istruzioni www.legalmail.it) per le altre tipologie di caselle

Attenzione: nel caso il titolare disponga della password per accedere alla casella, è disponibile la funzione di cambio password tramite le opzioni dell'interfaccia Webmail.

6. Accesso al servizio

Per accedere alla casella di posta elettronica Legalmail, l'utente può utilizzare il proprio client di posta elettronica. E' inoltre disponibile, in aggiunta alla modalità standard, l'accesso con un browser Internet collegandosi all'applicazione Webmail tramite il sito <http://pec.andi.it> e quindi alla casella di posta.

L'accesso alla casella di posta Legalmail, sia con client sia via Webmail, 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).

Per il client, utilizzabile via POP3 e IMAP, è necessario come versione minima: Outlook Express 5.5, o prodotti equivalenti/superiori.

Per il browser è necessario come versione minima Internet Explorer 5.5, o prodotti equivalenti/superiori, per utilizzare le funzionalità complete di firma, crittografia con il protocollo sicuro https.

6.1 Accesso via Webmail

Per motivi di sicurezza il cliente DEVE provvedere subito al cambio della 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, in caso di inutilizzo, 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. In tal caso deve provvedere alla apertura di una nuova sessione di lavoro.

6.2 Accesso via client

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.

7. Raccomandazioni generali

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 (100 MB complessivi) e quindi i messaggi successivi vengano rifiutati.

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.

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 a valore legale, costituisce una garanzia anche per i destinatari.

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

8. Dimensioni casella e messaggi

La dimensione di una casella è di 100 MB.

Si ricorda che la massima dimensione complessiva di un messaggio è pari a 45 MB. E' possibile inviare o ricevere un messaggio con allegati di peso complessivo fino a 30 MB.

I sistemi di posta elettronica trasformano gli allegati per permetterne la trasmissione e questo fa aumentare la dimensione del messaggio inviato. Questo significa che un messaggio con un allegato di 100KB potrebbe diventare durante la spedizione di 135 KB (il rapporto non è costante, si tratta di un puro esempio).

Per messaggi di grandi dimensioni, viene garantito l'invio nel caso in cui il prodotto della dimensione del messaggio per il **numero di destinatari diretti (to) di posta certificata**, non superi i 45 MB (e quindi in cui il peso complessivo degli allegati non superi i 30 MB).

Nel caso in cui il prodotto così ottenuto superi il valore di soglia, il sistema non accetterà il messaggio notificando l'evento all'utente tramite il relativo messaggio di 'Avviso di non accettazione'.

E' buona norma, prima di spedire un messaggio di dimensioni significative, 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 deve essere disponibile, pertanto, nella propria casella mittente lo spazio sufficiente. In caso contrario, le ricevute eccedenti la dimensione della casella non saranno recapitate.

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

E' responsabilità dell'utente la verifica dello stato di riempimento della propria casella PEC, e il suo periodico svuotamento.

Il sistema provvede a notificare il riempimento della casella oltre soglie predefinite. In particolare è previsto un avviso al superamento del 70%

XY`c`gdUn]c`X]gdc b]V]`Y"