

POSTA ELETTRONICA CERTIFICATA

Descrizione del servizio



SOMMARIO

1) Cosa è la Posta Certificata	3
2) Come funziona la Posta Certificata	4
3) Cosa acquista il Cliente	6
3.1 Dominio di Posta Certificata	7
3.1.1 Domini certificati di BPR	7
3.1.2 Dominio o sottodominio del Cliente	7
3.2 Modalità di utilizzo	8
4) Ripartizione delle attività	8
5) Identificazione dei titolari delle utenze di posta certificata	9
5.1 Informativa sugli obblighi del Titolare	9
5.2 Informativa sulla Privacy	9
5.3 Invio della documentazione	10



1) Cosa è la Posta Certificata

La Posta Certificata si inserisce nella più ampia gamma di servizi e prodotti che BPR realizza rivolti alla soddisfazione delle esigenze di sicurezza nella trasmissione e nello scambio di dati, che ormai caratterizzano i flussi di comunicazione digitale.

L'uso sempre più frequente della posta elettronica in sostituzione dei tradizionali mezzi di comunicazione e trasferimento dati e messaggi, insieme alla necessità di dare rilievo legale ai documenti informatici e al loro trasferimento richiedono un sistema **affidabile, sicuro** capace di fornire le **garanzie richieste dalle norme in materia di formazione e trasferimento dei documenti informatici**.

La posta elettronica tradizionale, infatti, presenta ancora numerose lacune relativamente allo scambio di dati tra il mittente ed il destinatario di una comunicazione, perché non garantisce:

- la riconoscibilità del mittente;
- la protezione (integrità ed inalterabilità del messaggio);
- la privacy (riservatezza del messaggio);
- la consegna;
- il non ripudio (valore legale della comunicazione).

I servizi di posta certificata colmano queste lacune per fornire agli utenti un servizio capace di sostituire integralmente il tradizionale servizio di posta (elettronica e cartacea). La posta certificata, infatti, permette di:

- garantire che il messaggio proviene da un gestore di posta e da uno specifico indirizzo e-mail (**riconoscibilità** del mittente);
- assicurare l'inalterabilità del messaggio durante la trasmissione (**protezione** del messaggio);
- effettuare lo scambio di dati in un ambiente al sicuro dall'intromissione di soggetti non autorizzati (**privacy** della comunicazione);
- fornire al mittente la prova dell'avvenuto recapito dell'e-mail alla casella di posta certificata destinataria tramite una ricevuta di consegna, esattamente come avviene con la tradizionale raccomandata A/R e con lo stesso valore legale (**garanzia di consegna e non ripudio** della destinazione);
- garantire il destinatario contro eventuali messaggi non ricevuti e di cui il mittente sostiene l'invio (**non ripudio** dell'origine);
- **attestare** in modo inequivocabile **la data di consegna/ricezione del messaggio** e la traccia dello scambio avvenuto.

Occorre in ogni caso tenere presente che il livello delle garanzie appena descritte varia a seconda della tipologia di posta elettronica fra le quali avviene lo scambio dei messaggi. Le ipotesi da considerare sono le seguenti:

- **mittente** e **destinatario** utilizzano un account certificato;
- solo il **mittente** utilizza un account di posta certificata.



La tabella che segue illustra le implicazioni delle due fattispecie:

Ipotesi	Livello di garanzia
Sia il mittente che il destinatario utilizzano un account di posta certificata	<ul style="list-style-type: none"> • È l'equivalente della tradizionale raccomandata A/R. • Il mittente dispone della ricevuta di avvenuta spedizione (proprio server certificato) e della ricevuta di avvenuta consegna del messaggio (server certificato del destinatario).
Solo il mittente utilizza un account di posta certificata	<ul style="list-style-type: none"> • È equivalente al tradizionale servizio di posta cartacea con ricevuta della spedizione. • Il mittente dispone della ricevuta di avvenuta spedizione (proprio server certificato), ma non dispone della ricevuta di avvenuto recapito del messaggio.

Con la Posta Certificata di BPR i clienti hanno a loro disposizione uno strumento di invio della documentazione riservata e dei dati sensibili in formato digitale che dà la **garanzia assoluta della sicurezza del mezzo** (integrità del messaggio e riservatezza), **della consegna del messaggio al destinatario** e **del tracciamento della spedizione**.

L'integrazione della Posta Certificata con gli altri servizi di sicurezza proposti da BPR consente di:

- Garantire **integrità, riservatezza e non ripudio** dei dati trasmessi utilizzando certificati residenti su smart card o sulla postazione dell'utente (Key-Ring);
- **Identificare con certezza** l'utente che accede alla casella di posta del servizio mediante un certificato di autenticazione;
- **Firmare elettronicamente** i messaggi inviati;
- **Cifrare** i messaggi inviati (ove consentito dal client);
- Nell'utilizzo del servizio viene garantita la compatibilità dei certificati X.509 e delle SmartCard con i seguenti prodotti client: Internet Explorer, Outlook, Netscape Communicator, Netscape Messenger.

2) Come funziona la Posta Certificata

Le *Linee Guida del servizio di trasmissione di documenti informatici mediante posta elettronica certificata* ed il relativo Allegato Tecnico, emessi dal Centro Tecnico per la Rete Unitaria della Pubblica Amministrazione¹, definiscono nel dettaglio le modalità attraverso le quali avviene lo scambio di messaggi di posta certificata e le regole per l'interoperabilità tra gestori. Gli **attori** principali che intervengono nel funzionamento di un sistema di Posta elettronica certificata sono il **mittente** ed il **destinatario**, con i relativi client di posta; ulteriori elementi che compongono il sistema sono:

¹ Ora CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione



- **il punto di ricezione**, ovvero l'infrastruttura che permette lo scambio di messaggi di posta certificata tra diversi gestori di posta certificata e che consente l'inserimento di messaggi di posta elettronica ordinaria nel circuito della posta certificata;
- il Server di Posta Certificata mittente, ovvero il **punto di accesso**;
- il Server di Posta Certificata destinatario, ovvero il **punto di consegna**.

Il processo di scambio dei messaggi di posta certificata, avviene secondo le fasi seguenti:

1 - Invio del messaggio da parte del mittente

Il **mittente** invia un messaggio attraverso il servizio di posta certificata. Il server di posta certificata del mittente (**punto di accesso**) esegue una serie di controlli formali sul messaggio pervenuto e provvede a generare una ricevuta di accettazione. I controlli formali accertano se i destinatari del messaggio appartengono all'infrastruttura di posta certificata o sono utenti esterni (es. posta Internet).

Prosegue poi "imbustando" il messaggio originale in un messaggio di trasporto ed inviando al mittente una ricevuta di accettazione, con la quale conferma al mittente che il suo messaggio è stato accettato dal sistema, ad una data e ora specifiche.

La **ricevuta di accettazione** è un messaggio di posta elettronica firmato dal gestore del mittente, nel quale sono riportati la data ed ora di accettazione, l'oggetto ed i dati del mittente e del destinatario. Nella ricevuta di accettazione è riportata la tipologia dei vari destinatari per informare il mittente del differente flusso seguito dai due gruppi di messaggi.

Il messaggio di trasporto firmato dal gestore del mittente, è un messaggio che contiene, come allegato, il messaggio originale e tutti i dati che ne certificano il trasporto. Il messaggio di trasporto viene quindi inviato al mittente attraverso il punto di ricezione.

2 - Invio del messaggio al punto di ricezione

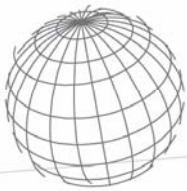
All'arrivo di un messaggio, il **punto di ricezione** ne verifica la natura e la corretta composizione. In particolare, il punto di ricezione verifica l'esistenza e la validità della firma del gestore che ha consegnato il messaggio del mittente. Se le verifiche sono positive, emette una **ricevuta di presa in carico** verso il gestore mittente e provvede ad inoltrare il messaggio ricevuto verso il punto di consegna.

3 - Invio del messaggio al punto di consegna

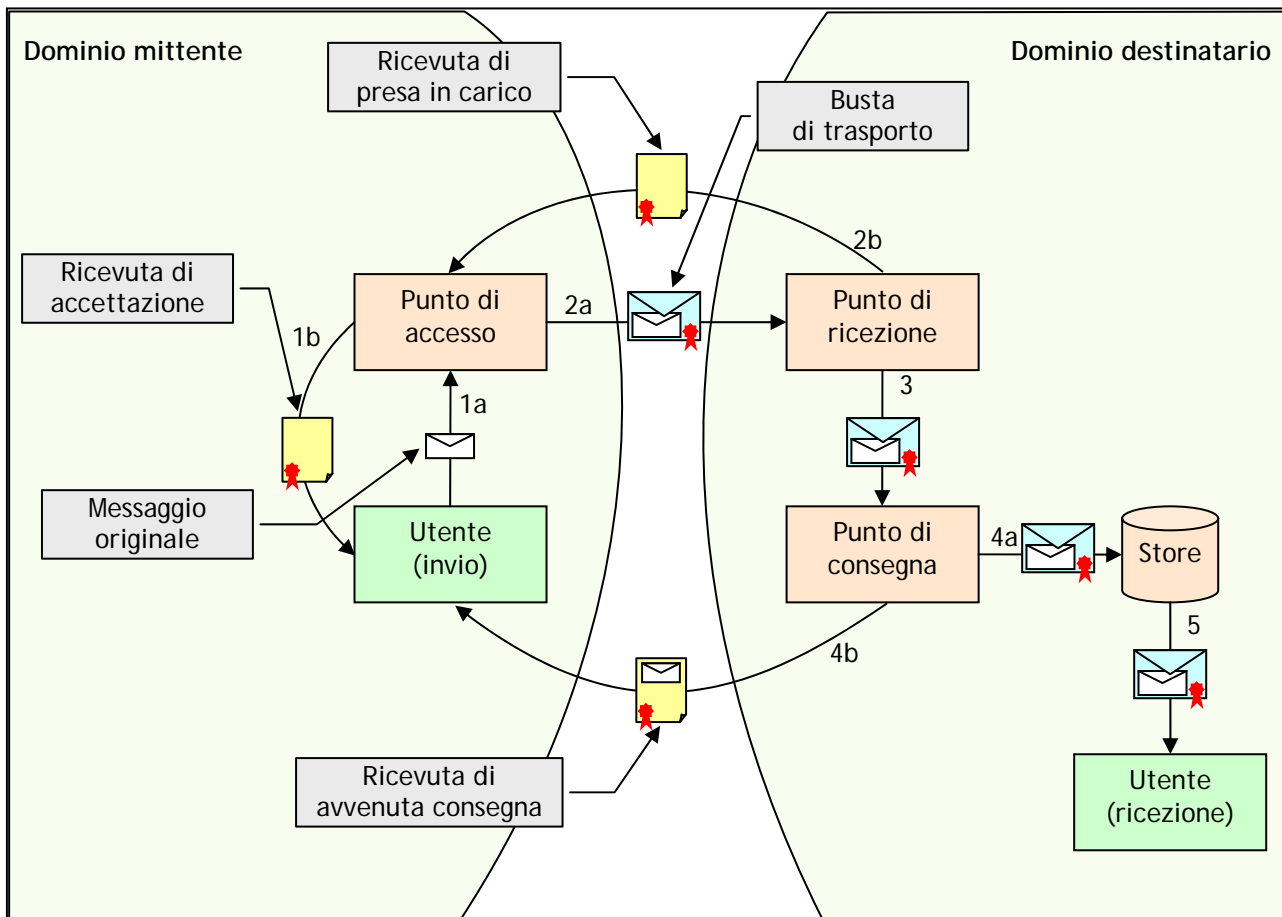
Quando il messaggio di trasporto è stato consegnato al server di posta del destinatario (**punto di consegna**), questo emette ed invia al mittente una **ricevuta di avvenuta consegna**, che conferma al mittente che il suo messaggio è stato effettivamente consegnato al destinatario specificato, certificando la data e l'ora dell'evento. L'emissione della ricevuta di avvenuta avviene contestualmente alla disponibilità del messaggio nella casella di posta elettronica del destinatario, indipendentemente dalla lettura da parte sua.

4 - Problemi nel trasporto

La situazione appena descritta costituisce la normalità dei casi, ma si possono verificare delle situazioni nelle quali qualche cosa non va per il verso giusto. In tutti i casi di questo tipo, viene generato un **messaggio di anomalia di trasporto** (contenente il messaggio che



non ha superato i controlli) inoltrato al punto di consegna. Inoltre, nel caso in cui il messaggio pervenuto al punto di consegna non fosse recapitabile alla casella di destinazione, il punto di consegna emette una ricevuta di **errore di consegna** da restituire al mittente con l'indicazione dell'errore riscontrato.



3) Cosa acquista il Cliente

Il servizio di Posta Certificata offerto al cliente si differenzia sulla base delle diverse possibili combinazioni dei seguenti elementi:

- **Dominio sul quale sono configurate le caselle di posta elettronica:** di IT Telecom o del Cliente
- **Tipologia di servizio:** casella privata, casella istituzionale
- **Modalità di utilizzo:** webmail o clienti di posta
- **Possibilità di personalizzazione dell'interfaccia.**

Per quanto riguarda gli utilizzatori, è invece possibile distinguere tre profili di utenza:



Il primo profilo fa riferimento ad un insieme di clienti prevalentemente formato da **utenze residenziali, micro business e professionisti**, che utilizzano saltuariamente la posta certificata. Prevalentemente lo faranno in sporadici scambi di corrispondenza fra loro, o verso gli Enti della PA.

Il secondo profilo si riferisce agli **Enti della PA**, a partire da quelli di dimensioni medio piccole e alle **imprese**, a partire da quelle di dimensioni medie, che utilizzano in modo intensivo e consistente la Posta Certificata nell'ambito delle relazioni fra loro ed i loro referenti. Nel caso della PA, si fa riferimento alle Aree Organizzative Omogenee che ogni ente dovrà costituire per lo scambio della posta certificata; mentre nel caso delle imprese, si fa riferimento alle strutture funzionali che sono maggiormente interessate alla tematica (le funzioni legali, le funzioni acquisti, le funzioni commerciali, ecc.)

Il terzo profilo si riferisce a **micro business, piccole imprese, professionisti e gli enti più piccoli della PA**, che hanno esigenze continuative di utilizzare la posta certificata, ma con flussi di traffico meno complessi, comunque collegati a tipi organizzativi più semplici.

3.1 Dominio di Posta Certificata

3.1.1 *Domini certificati di BPR*

In questo caso il cliente, invece di utilizzare un proprio dominio Internet per la gestione della sua corrispondenza certificata, si appoggia al dominio di Posta Certificata del BPR.

Tutti gli scambi in entrata ed in uscita effettuati dalle caselle di posta del cliente configurate in questo dominio, sono trattati come scambi di messaggi di posta certificata. Coerentemente alla normativa vigente assumono quindi un valore equivalente alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Per ogni messaggio inviato, il mittente riceverà una ricevuta di accettazione ed una ricevuta di consegna per ciascuno dei destinatari ai quali il messaggio è stato inviato (in caso di problemi di consegna o anomalie nell'utilizzo del servizio, riceverà le corrispondenti ricevute di errore).

3.1.2 *Dominio o sottodominio del Cliente*

In questa ipotesi, il cliente che già possiede un suo dominio o un sottodominio Internet, ne chiede la configurazione come dominio o sottodominio di posta certificata.

Tutti gli scambi in entrata ed in uscita effettuati dalle caselle di posta del cliente configurate nel dominio certificato sono trattati come scambi di messaggi di posta certificata. Coerentemente alla normativa vigente assumono quindi un valore equivalente alla notificazione per mezzo della posta nei casi consentiti dalla legge. Per ogni messaggio inviato, il mittente riceverà una ricevuta di accettazione ed una ricevuta di consegna per ciascuno dei destinatari ai quali il messaggio è stato inviato (in caso di problemi di consegna o anomalie nell'utilizzo del servizio, riceverà le corrispondenti ricevute di errore).

Rispetto al caso del dominio di posta certificata BPR, in questo caso il *maintainer* del DNS del cliente è tenuto a curare la relativa configurazione, per assicurare la visibilità



in rete dei server coinvolti nel processo di certificazione. BPR, da parte sua, verificherà che l'azienda che richiede la certificazione del dominio ne sia effettivamente titolare e che il dominio sia regolarmente registrato.

È importante tenere presente che, anche nel caso di dominio o sottodominio del cliente, i servizi relativi al dominio certificato verranno comunque erogati dalla piattaforma BPR.

3.2 Modalità di utilizzo

La soluzione di Posta Elettronica Certificata IT Telecom prevede la possibilità di **sfruttare tutte le funzionalità di gestione delle caselle di posta** – siano esse istituzionali o individuali – **attraverso un normale web browser o** potranno accedere a tutte le funzionalità della loro casella di posta anche utilizzando un normale client di posta - come ad esempio Microsoft Outlook, Outlook Express o Netscape Messenger - adeguatamente configurato².

4) Ripartizione delle attività

Per l'attivazione del servizio di Posta Elettronica Certificata sono previste le attività seguenti:

- Il **network manager del Cliente** provvede a configurare i firewall in modo da consentire il passaggio dei protocolli standard richiesti dal servizio di posta.
- Il **Cliente** provvede ad **identificare personalmente tutti gli utenti** del servizio di posta certificata, attraverso un suo *Incaricato all'identificazione*³, delegato da BPR a questa attività.
- Il **Cliente** comunica la lista nominativa delle persone per le quali richiede l'attivazione delle caselle di posta certificata e delle eventuali utenze supplementari per l'accesso alle caselle istituzionali, in modo che sia chiaramente associato alla singola casella utilizzata il nome della persona che la utilizzerà, come richiesto dalla normativa vigente.
- **BPR** cura la configurazione e l'attivazione delle caselle di posta richieste.

Una volta completate queste attività relative all'attivazione, occorre effettuare le seguenti operazioni di *provisioning* per consentire agli utenti di sfruttare il servizio. In particolare: L'incaricato dell'identificazione provvede ad assegnare le **credenziali di accesso al servizio** (*userid* e *password*) agli utenti.

Se l'utente si avvale di un client di posta, dovrà effettuare la **configurazione**.

Solo nel caso di dominio del cliente dovranno inoltre essere svolte le seguenti attività, ai fini dell'attivazione:

BPR verifica se l'azienda che richiede la certificazione del dominio ne sia effettivamente titolare e che il dominio sia regolarmente registrato.

Il **maintainer del DNS** del cliente cura la sua configurazione per assicurare la visibilità in rete dei server coinvolti nel processo di certificazione.

² Per la configurazione del client di posta si rimanda al documento: "Posta Elettronica Certificata – Configurazione del client di posta".

³ Normalmente è un dipendente dell'azienda cliente, che funge da punto di raccordo tra l'azienda cliente ed BPR. L'incaricato dell'identificazione dovrà essere a sua volta identificato da un funzionario BPR.



5) Identificazione dei titolari delle utenze di posta certificata

Per accedere al servizio di posta certificata, gli utenti devono essere preventivamente identificati. Le informazioni relative a questi soggetti sono registrate nel sistema di posta certificata **utilizzando le funzionalità previste dal portale PKI**. L'Incaricato dell'Identificazione è un soggetto delegato con un apposito atto da BPR, per le attività di **identificazione degli utenti del servizio di posta certificata**.

Al fine di consentire il corretto svolgimento della procedura di identificazione, le persone che richiedono un'utenza di posta certificata devono **presentarsi all'Incaricato dell'identificazione**, recando con sé:

- una carta di identità italiana in corso di validità, oppure un documento equipollente munito di fotografia e rilasciato da una Amministrazione dello Stato⁴.
- il tesserino rilasciato dal Ministero delle Finanze contenente il Codice Fiscale.

All'atto dell'identificazione, l'incaricato **controlla che il documento fornito dal Richiedente sia autentico e privo di segni visibili di contraffazione**; anche se la garanzia in merito all'autenticità del documento non rientra nelle competenze dell'Incaricato dell'Identificazione, infatti, è compito di quest'ultimo operare una valutazione che consenta un ragionevole affidamento sulla validità e autenticità dello stesso. In particolare, qualora l'incaricato dell'identificazione abbia dei dubbi sulla validità o sulla autenticità del documento presentato dal richiedente, può chiedere a quest'ultimo di fornire un altro documento di riconoscimento. Una volta accertate validità ed autenticità del documento fornito l'incaricato chiede al richiedente di presentare il tesserino con il codice fiscale.

5.1 Informativa sugli obblighi del Titolare

Accertata l'identità del richiedente come descritto nel paragrafo precedente, l'incaricato dell'identificazione è tenuto ad informarlo, prima di inserire i dati identificativi dello stesso nel sistema informativo, sui necessari requisiti tecnici per accedere al portale. L'Incaricato dell'Identificazione dovrà inoltre informare il richiedente degli obblighi che questi assume in merito alla protezione della segretezza delle credenziali di accesso al servizio. In particolare deve informarlo dell'obbligo di informare BPR di ogni variazione delle informazioni fornite durante la procedura di identificazione e registrazione.

5.2 Informativa sulla Privacy

L'Incaricato dell'Identificazione è tenuto ad informare il richiedente sulle modalità di gestione dei suoi dati personali, nel rispetto della vigente normativa in materia di riservatezza e trattamento dei dati personali. A tal fine deve fornire al richiedente il modulo "Informativa resa all'interessato per il trattamento dei dati personali" e assicurarsi che il ri-

⁴ Passaporto italiano, Patente auto, Tessere di riconoscimento del personale delle amministrazioni statali, Porto d'armi, Tessere di riconoscimento rilasciate dai Paesi appartenenti alla UE, Permesso di soggiorno (per cittadini stranieri).



chiedente prenda visione dell'informativa e la sottoscriva, dando il suo consenso al trattamento dei dati personali.

5.3 Invio della documentazione

Una volta terminata la fase di identificazione e di registrazione del richiedente, l'Incaricato dell'Identificazione dovrà raccogliere e organizzare tutta la documentazione, che dovrà poi essere inoltrata ad BPR ai fini dell'erogazione del servizio. L'Incaricato dell'Identificazione deve predisporre un plico, che dovrà contenere:

- a) La fotocopia di uno dei documenti di identità;
- b) Fotocopia del tesserino con il Codice Fiscale;
- c) Eventuale originale del documento comprovante i poteri di rappresentanza di persone fisiche o giuridiche, o di appartenenza agli ordini professionali;
- d) La stampa del "Modulo di registrazione del Titolare" firmato;
- e) Originale firmato del "Modulo di adesione al servizio di posta certificata".

L'incaricato dovrà quindi acquisire la documentazione per ogni account di posta elettronica certificata in formato elettronico PDF, firmare il file digitalmente ed inviarlo per posta elettronica certificata all'indirizzo email: registrazione@bprcert.it insieme ai documenti di cui ai punti c), d) ed e) firmati digitalmente dal cliente.

In caso il cliente non fosse in possesso di firma digitale, i documenti saranno conservati dall'incaricato temporaneamente che provvederà ogni 30 giorni ad inviare in unica busta le copie in originale dei documenti c), d) ed e).

Una volta che la busta sia stata chiusa, nessun altro segno identificativo deve essere apposto all'esterno della busta. Il plico contenente la documentazione di cui al paragrafo precedente deve essere spedito tramite raccomandata A/R o tramite corriere di posta celere con modalità che assicurino al mittente l'avvenuta ricezione del plico, al seguente indirizzo:

BPR s.r.l.
Piazza Carbone, 10
Servizio PEC
89015 PALMI (RC)

L'Incaricato dell'Identificazione dovrà inserire nel pacco anche una lista contenente il numero totale dei richiedenti ai quali si riferiscono.

Il pacco contenente i plichi dovrà a sua volta essere chiuso, riportare all'esterno, oltre all'indirizzo sopra indicato, anche la dicitura "Identificazione Titolari ed il nome della società o della pubblica amministrazione di appartenenza".