
PostaCertificat@

Guida Pubblica Amministrazione

1 Che cos'è PostaCertificat@

La PostaCertificat@ (Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino) è un servizio di comunicazione elettronica sicuro e certificato tra Pubblica Amministrazione e Cittadino.

Il servizio è offerto a titolo gratuito e si rivolge:

1. a tutti i cittadini italiani maggiorenni che ne facciano richiesta;
2. a tutte le amministrazioni pubbliche locali e centrali per i propri registri di protocollo, utilizzati per le comunicazioni tra Pubblica Amministrazione e Cittadino

La PostaCertificat@ garantisce un canale di comunicazione tra Pubbliche Amministrazioni e tra Pubblica Amministrazione e Cittadino, non sono, infatti, previste comunicazioni al di fuori di tali canali, ad esempio tra Cittadino e Cittadino. Tale strumento di comunicazione:

- o fornisce tutte le garanzie di una posta elettronica certificata;
- o permette di dare ad un messaggio di posta elettronica la piena validità legale nei casi previsti dalla normativa;
- o garantisce data e ora riferiti all'accettazione e alla consegna del messaggio e l'integrità del contenuto trasmesso.

La PostaCertificat@ è rilasciata ai sensi dell'art. 16-bis del Decreto Legge del 29 novembre 2008, n. 185, recante "Misure occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale", convertito in legge del 28 gennaio 2009, n. 2 e del Decreto del Presidente del Consiglio dei Ministri del 6 maggio 2009 recante disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata ai cittadini.

L'utilizzo della PostaCertificat@ avviene ai sensi del Codice dell'Amministrazione Digitale ed è aderente al Regolamento sulla Posta Elettronica Certificata DPR 11 febbraio 2005, n. 68 ed alle Regole Tecniche di cui al Decreto Ministeriale 2 Novembre 2005.

2 I servizi della PostaCertificat@ per la Pubblica Amministrazione

2.1 Servizi base per la Pubblica Amministrazione

I servizi base, ossia l'insieme dei servizi necessari a garantire la creazione di un canale di comunicazione semplice, diretto e sicuro tra Cittadino e Pubblica Amministrazione - sono:

1. la fornitura di **caselle di posta elettronica PostaCertificat@** per i propri registri di protocollo, con dimensione di 500 MB per ogni casella attivata;
2. l'elenco degli **indirizzi dei cittadini che hanno aderito al servizio PostaCertificat@**
3. il **registro delle operazioni**, cioè l'archivio informatico delle operazioni effettuate
4. **invio massivo** delle comunicazioni ai cittadini.

2.2 Servizi avanzati per la Pubblica Amministrazione

Verranno forniti alle Pubblica Amministrazione ulteriori servizi, a pagamento, quali:

- PA Front Office (sportello virtuale PA per il cittadino)
- PA Folder (backup e gestione documentale)
- Gestione modulistica elettronica
- Servizio Mail Room – Piattaforma di Gestione Elettronica Documentale
- Servizio di marcatura elettronica del documento

Ciascuna Pubblica Amministrazione potrà richiedere l'attivazione dei servizi avanzati, selezionando sulla sezione dedicata del portale i servizi di proprio interesse.

3 Come la Pubblica Amministrazione può richiedere la casella PostaCertificat@ (protocollo)

Ciascuna Pubblica Amministrazione potrà visualizzare nella sezione informativa del portale www.postacertificata.gov.it le istruzioni per richiedere il servizio PostaCertificat@.

Di seguito le attività necessarie per richiedere la Casella PostaCertificat@:

1. Nella sezione informativa del Portale dedicata alla Pubblica Amministrazione, sono presenti le **Condizioni Generali del Servizio** (CGS PA), il **Modulo di Adesione** del servizio e **l'allegato 1, Modulo Richiesta attivazione Caselle Protocollo PA**, che ciascuna Amministrazione dovrà scaricare e compilare nei campi necessari.
2. Tali moduli, una volta compilati, dovranno essere firmati dal referente della singola Pubblica Amministrazione dotato dei necessari poteri di firma. Inoltre, dovrà essere individuato ed indicato l'Amministratore del servizio PostaCertificat@ (qualora diverso dal firmatario). La Pubblica Amministrazione sottoscrittore dovrà inoltre predisporre la seguente documentazione:
 - Fotocopia del documento di identità del firmatario;
 - Delibera/determina emessa dalla Pubblica Amministrazione che ratifichi il potere di firma del firmatario;
 - Fotocopia del documento di identità dell'amministratore del servizio (se diverso dal firmatario)
 - Elementi di contatto dell'amministratore del servizio (indirizzo, e.mail, rif. Telefonici)
 - Numero ed elenco delle caselle protocollo PostaCertificat@ da attivare, secondo il form presente sul portale www.postacertificata.gov.it
3. Una volta completato la preparazione dei documenti di cui al punto precedente, ciascuna Pubblica Amministrazione potrà scegliere tra tre diverse modalità di attivazione del servizio PostaCertificat@ messe a disposizione dal Concessionario:
 - A Invio del Modulo di adesione e degli allegati all'indirizzo mail postacertificata_pa@posteitaliane.it **del Centro Servizi Amministrativi del Concessionario firmati digitalmente dalla Pubblica Amministrazione sottoscrittore** (caso in cui la Pubblica Amministrazione sia dotata di firma digitale);

- B consegna del modulo di adesione e degli allegati presso l'Ufficio Postale abilitato** più vicino (vedi elenco presentato sul Portale www.postacertificata.gov.it)
- B.1) In questo caso la consegna della documentazione dovrà essere effettuata dal firmatario dei Moduli e/o dall'Amministratore del servizio PostaCertificat@ individuato nel modulo di adesione stesso presentando all'operatore un proprio documento di identità. L'operatore dell'ufficio postale effettua la verifica di congruità tra i dati del documento di identità presentato ed i dati di identificazione (fotocopia del documento di identità) allegati al modulo di adesione presentato allo sportello; l'operatore quindi timbra, per presa visione, la copia del modulo di adesione e predispone un fax di tutta la documentazione sopra elencata inviandola al numero **06-98688002** del Centro Servizi Amministrativi del concessionario.
- C contatto (qualora presente) con il proprio responsabile commerciali del Concessionario:** in questo caso sarà cura del responsabile commerciale del Concessionario, concordata l'adesione al servizio con la PA sottoscrivente, predisporre l'invio via fax della documentazione al numero **06-98688002** o postacertificata_pa@posteitaliane.it del Centro Servizi Amministrativi del Concessionario.
4. Indipendentemente dal canale utilizzato dalla Pubblica Amministrazione per l'invio del modulo di adesione e di tutta la documentazione richiesta, la documentazione viene presa in carico dall'operatore del **Centro Servizi Amministrativi** che effettua, per ciascuna pratica, le seguenti attività:
- verifica della completezza e dell'accuratezza dei dati inseriti e di tutta la documentazione;
 - data entry delle informazioni previste per l'attivazione delle caselle protocollo, secondo quanto richiesto (All.1- Modulo Richiesta di Attivazione Caselle Protocollo Pubblica Amministrazione);
 - invio del file al Supporto Tecnico per l'attivazione delle caselle
 - invio della documentazione cartacea presso il centro per l'archiviazione
- N.B.** Nel caso in cui le verifiche siano negative, l'operatore del Centro Servizi Amministrativi provvederà a contattare l'Amministratore del servizio della Pubblica Amministrazione/responsabile commerciali del Concessionario al fine di sanare le anomalie riscontrate.
5. **Il supporto tecnico del Concessionario completa** la fase di attivazione delle caselle PostaCertificat@ ed invia le credenziali all'Amministratore del servizio PostaCertificat@ all'indirizzo di posta elettronica indicato nel modulo di adesione. L'attivazione avverrà entro 5 gg dalla data di invio/trasmissione/consegna della documentazione nei vari canali sopra indicati.
6. **Al primo accesso**, l'Amministratore Pubblica Amministrazione utilizza le credenziali di accesso ricevute e **modifica la password** inserita.

N.B. Per attivare ulteriori nuove Caselle protocollo Pubblica Amministrazione, l'Amministratore del servizio dovrà inviare dalla propria casella PostaCertificat@ il **Modulo Richiesta Attivazione Caselle Protocollo Pubblica Amministrazione**, presente nel portale www.postacertificata.gov.it, all'indirizzo

postacertificata_pa@posteitaliane.it del Centro Servizi Amministrativi del Concessionario. L'attivazione delle ulteriori caselle protocollo richieste dall'Amministratore del servizio avverrà entro 5 gg dalla data di invio/trasmissione/consegna della documentazione.

4 Le Caselle PostaCertificat@

Le caselle PostaCertificat@ offerte a titolo gratuito a tutte le Amministrazioni che ne facciano richiesta, rispondono alle *Regole Tecniche sulla Posta Elettronica Certificata*.

In dettaglio le caratteristiche peculiari della Casella PostaCertificat@ sono:

1. la certificazione della data e dell'ora dell'invio e della consegna del messaggio e dei contenuti allegati,
2. la garanzia sull'integrità del contenuto delle comunicazioni rispetto a modifiche non autorizzate,
3. l'opponibilità a terzi delle evidenze relative alle operazioni di invio e consegna dei messaggi,
4. la gestione e l'archiviazione dei log relativi alle comunicazioni.

La dimensione delle singole Caselle PostaCertificat@ fornite alla Pubblica Amministrazione è pari a 500MB.

4.1 Cosa è possibile fare con la Casella PostaCertificat@

Una volta effettuata l'autenticazione l'utente potrà:

- o visualizzare la lista dei messaggi in arrivo;
- o selezionare e leggere un singolo messaggio;
- o selezionare e cancellare uno o più messaggi;
- o scrivere un nuovo messaggio;
- o selezionare ed inoltrare un messaggio ricevuto;
- o selezionare e rispondere ad un messaggio ricevuto.

Accedendo alla casella, l'utente Pubblica Amministrazione potrà anche predisporre un "invio massivo" di comunicazioni verso i Cittadini, a partire dalla rubrica, creando liste personalizzate dalle quali selezionare i destinatari o l'intera lista creata.

5 Come modificare i propri dati

5.1 Come cambiare la password al primo accesso

L'Amministratore del servizio di PostaCertificat@ e gli utenti delle singole caselle di registro possono cambiare la propria password in qualsiasi momento attraverso le funzionalità di modifica password accessibile attraverso il portale web.

L'utente della Casella accede alla Home Page del portale e alla sua Area Privata inserendo User-Id e Password.

5.2 Modifica password

Per modificare la password il portale richiede di inserire direttamente la nuova password prescelta e di confermarla. Al termine dell'inserimento della nuova password l'utente dovrà eseguire il salvataggio della nuova password inserita.

5.3 Modifica dati

Per modificare i dati forniti per l'attivazione del servizio, l'Amministratore del servizio di PostaCertificat@ dovrà inviare alla casella centroservizi@postacertificata.gov.it il modulo **Modifica Dati PA e Caselle Protocollo**, presente sul portale www.postacertificata.gov.it.

Il modulo dovrà essere inviato mediante la casella PostaCertificat@ della Pubblica Amministrazione e dovrà essere compilato nelle sezioni che si intendono aggiornare.

6 Come recedere dal servizio PostaCertificat@

Per recedere dal servizio, l'Amministratore del servizio di PostaCertificat@ dovrà inviare alla casella centroservizi@postacertificata.gov.it il modulo **Recesso dal servizio - Pubblica Amministrazione**, presente sul portale www.postacertificata.gov.it.

Il modulo dovrà essere inviato mediante la casella PostaCertificat@ della Pubblica Amministrazione e dovrà essere compilato nelle sezioni dedicate.

Qualora la Pubblica Amministrazione decida di recedere dal servizio è importante che la stessa effettui un salvataggio dei propri dati presenti nel sistema PostaCertificat@ prima dell'inoltro richiesta recesso.

Qualora ciò non avvenisse la Pubblica Amministrazione recedente potrebbe incorrere nella perdita dei propri dati.

7 Sicurezza

Le funzionalità che garantiscono la sicurezza delle comunicazioni effettuate attraverso Postacertificat@ sono le seguenti:

- canale di trasmissione sicura;
- gestione dei virus informatici;
- tracciabilità e log dei messaggi;
- riservatezza.

8 Requisiti della postazione

I requisiti minimi per accedere ai servizi PostaCertificat@ sono i seguenti:

- o connessione a internet;
- o client di posta elettronica o web browser;
- o capacità di connettersi alle porte standard e compatibilità con i protocolli seguenti:
 1. HTTPS 443 per accedere alla casella PostaCertificat@ ed alle sezioni private del Portale Web;
 2. SMTP/S porta 465 per invio di messaggi;
 3. IMAP/S porta 993 per ricezione posta con client;
 4. POP3/S porta 995 per ricezione posta con client.

9 Configurazione client di posta elettronica

Nel caso di utilizzo di un **Client di posta**, i valori di configurazione del client per la casella PostaCertificat@ sono:

1. **Server posta in arrivo:** mail.postacertificata.gov.it
 - **protocollo pop3:** il server richiede una connessione crittografata (ssl) porta 995
 - **protocollo imap:** il server richiede una connessione crittografata (ssl) porta 993
2. **Server posta in uscita:** mail.postacertificata.gov.it
 - **protocollo smtp:** il server richiede una connessione crittografata (ssl) porta 465
 - **attivare la funzione:** "Server della posta in uscita - Autenticazione del server necessaria"

10 Limitazioni all'utilizzo della casella PostaCertificat@

Il servizio di comunicazione PostaCertificat@ offerto consente le sole comunicazioni tra Cittadino e Pubblica Amministrazione e viceversa e tra caselle di PostaCertificat@ delle Pubbliche Amministrazioni.

Per le Caselle della Pubblica Amministrazione è esclusa totalmente la possibile interazione fra la casella PostaCertificat@ verso qualsiasi dominio di posta elettronica tradizionale.

11 Assistenza

Per poter avere informazioni sul servizio, la Pubblica Amministrazione potrà:

- visitare il Portale Web, www.postacertificata.gov.it
- contattare il Call Center accessibile da 800.104.464 (da rete fissa) - 199.135.191 (da rete mobile) disponibile dalle 8:00 alle 20:00, dal lunedì al sabato
- contattare (qualora presente) il proprio responsabile commerciale del Concessionario

12 Altri servizi Base per la Pubblica Amministrazione

12.1 *Elenco degli indirizzi dei cittadini abilitati a PostaCertificat@*

Sarà a disposizione della Pubblica Amministrazione un unico indirizzario che conterrà l'elenco aggiornato degli indirizzi PostaCertificat@ dei cittadini aderenti al servizio.

L'accesso a questo indirizzario è reso sicuro attraverso canali di trasmissione sicuri e previa autenticazione e autorizzazione, nel rispetto della disciplina in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n.196.

12.2 *Servizio di invio massivo*

Il servizio di Invio Massivo consente alla Pubblica Amministrazione l'invio agevole di messaggi di PostaCertificat@ in forma massiva, attraverso l'interazione con la rubrica e la creazione di liste personalizzate, al fine di veicolare messaggi verso i molteplici destinatari.

Queste comunicazioni massive potranno essere utilizzate per fornire informazioni di pubblica utilità a tutti i cittadini presenti nell'indirizzario a disposizione della Pubblica Amministrazione.

12.3 *Registro delle operazioni*

Il servizio PostaCertificat@ prevede per tutte le Pubbliche Amministrazioni una soluzione integrata che consente sia la gestione dei log nel rispetto di tutti i requisiti normativi in termini di raccolta e protezione dei log stessi, sia la realizzazione di una reportistica informativa di gestione del servizio.

Accedendo ad un'area dedicata del portale www.postacertificata.gov.it, ciascuna Pubblica Amministrazione avrà a disposizione una serie di report standard, che hanno l'obiettivo di fornire sia un sistema di Monitoraggio ed Analisi dei servizi in erogazione, sia analisi in merito all'adesione ai servizi.

L'accesso ai registri ed alle funzionalità di reportistica e analisi avviene attraverso una sezione opportuna e protetta del Portale Web.

12.4 *Ricevuta di presa visione (opzionale)*

In aggiunta alle ricevute e alle notifiche peculiari della Posta elettronica Certificata, il servizio PostaCertificat@ include, opzionale ai servizi Base, l'invio della ricevuta di presa visione nello scenario complessivo di comunicazione PostaCertificat@.

La ricevuta di presa visione viene generata, per notificare al mittente, nel caso sia anch'esso un utente PostaCertificat@ che il destinatario ha scaricato e/o consultato la e-mail dalla propria casella di posta elettronica certificata. Lo scenario prevede che sia il mittente che il destinatario abbiano caselle PostaCertificat@.

PostaCertificat@

Istruzioni per garantire la sicurezza della Casella

LA SICUREZZA DEL SERVIZIO PostaCertificat@

- **Limitazione delle comunicazioni** - il servizio di comunicazione PostaCertificat@ consente le sole comunicazioni tra Cittadino e PA e viceversa e quelle tra PA e PA, limitatamente alle caselle configurate/censite nel circuito PostaCertificat@
- **Canali di trasmissione sicuri** - tutte le connessioni sono realizzate tramite l'impiego di canali sicuri basati sull'utilizzo dei protocolli di trasporto Transport Layer Security (TLS)/Secure Sockets Layer (SSL), che permettono la crittografia dei dati trasmessi in rete.
- **Antivirus** - I sistemi di front-end che permettono il colloquio con i client e la webmail, includono componenti antivirus che effettuano controlli sia nei messaggi in ingresso, che in uscita. Le configurazioni adottate sono tali per cui tutti i messaggi di PostaCertificat@ in cui è rilevata la presenza di virus sono consegnati al motore di PostaCertificat@ per essere trattati in conformità alla normativa vigente.
- **Gestione Log** - Tutti i log inerenti i messaggi scambiati sono memorizzati su un registro (log) riportante i dati significativi dell'operazione. I log dei messaggi sono conservati per 30 mesi a cura del Gestore.
- **Integrità e limitazione dell'uso improprio del servizio** - il sistema PostaCertificat@ permette, attraverso le caratteristiche della piattaforma utilizzata, di tenere sotto controllo l'utilizzo delle risorse da parte dell'utente, sulla base di specifici parametri quali: il numero massimo di invii, la dimensione massima dei messaggi, numero massimo dei destinatari, dimensione massima dello spazio di memorizzazione della casella.

LA SICUREZZA DELLA POSTAZIONE UTENTE

L'attuazione di alcune regole comportamentali adottate nella gestione del personal computer assumono una importanza rilevante per la riduzione del rischio di malfunzionamenti nell'utilizzo del Servizio PostaCertificat@.

Nella normale gestione delle comunicazioni di una certa rilevanza, vanno tenute in considerazione le opportune regole di sicurezza per la postazione utilizzata al fine di trasmettere telematicamente, tra Pubblica Amministrazione e Cittadino, documenti informatici attraverso caselle PostaCertificat@.

Di seguito le principali regole di comportamento che è necessario osservare.

- La postazione di lavoro deve essere opportunamente configurata in modo che l'accesso ad essa avvenga solo previo inserimento di un "codice identificativo" (*nome utente*) e un "codice di accesso" (*password*). Il "codice di accesso" è da ritenersi strettamente personale e deve essere custodito in modo tale da evitarne la conoscenza a terzi non autorizzati all'accesso alla postazione. Inoltre, il "codice di accesso" deve essere non predicibile e rinnovato periodicamente.
- È molto importante proteggere la propria postazione di lavoro con l'utilizzo di un idoneo software Antivirus accertandosi che questo sia sempre attivo ed aggiornandolo periodicamente.
- In merito alle versioni e agli aggiornamenti del sistema operativo installato sulla postazione utente, accertarsi che il relativo servizio "Aggiornamenti automatici", qualora presente, sia attivo, oppure controllare periodicamente quanto disponibile sul sito ufficiale del fornitore del Sistema Operativo utilizzato ed eseguire gli aggiornamenti ad alta priorità segnalati.
- Se il PC è collegato ad una rete (Intranet o Internet) assicurarsi di aver preventivamente attivato il *personal firewall* già presente nei più recenti sistemi operativi commerciali. In mancanza di un *personal firewall* si consiglia di dotarsi di uno degli strumenti di mercato dedicati alla protezione della postazione.
- L'installazione di programmi di provenienza non fidata deve essere assolutamente evitata.
- Nell'utilizzo della posta elettronica, si raccomanda di non effettuare il *download* o l'apertura di file o prodotti di natura incerta e provenienti via posta elettronica da mittenti sconosciuti; tali file, generalmente di tipo ".EXE" o di tipo ".ZIP", possono essere portatori di programmi che compromettono la funzionalità della postazione di lavoro e di tutti gli applicativi installati; tra le misure precauzionali è, inoltre, buona norma disattivare la funzione di visualizzazione in anteprima dei messaggi in arrivo.
- Analogamente, nell'accesso a siti Internet si raccomanda di non effettuare il *download* o di eseguire programmi disponibili su Internet (generalmente di tipo ".EXE" o di tipo ".ZIP") dei quali non si conosca l'origine e lo scopo.

LA SICUREZZA NELL'UTILIZZO DELLA CASELLA PostaCertificat@

La casella PostaCertificat@ avvalendosi per l'accesso al servizio sia di strumenti messi a disposizione dal Concessionario che, anche client di posta elettronica tradizionale, presenta ulteriori regole di comportamento come di seguito sinteticamente riportate.

- Il Concessionario mette a disposizione, all'interno del Portale Web su un'area riservata, un'interfaccia webmail che permette l'accesso alla propria casella PostaCertificat@ tramite un comune browser utilizzando il protocollo sicuro SSL. Tale protocollo garantisce la sicurezza delle informazioni che vengono visualizzate e delle operazioni che vengono effettuate durante l'accesso alla propria casella o relative a scambi di informazione riservati (ad esempio per il cambio password).
- Per accedere al servizio PostaCertificat@, l'utente deve essere dotato di una postazione con accesso a internet, web browser e/o client di Posta Elettronica. La postazione deve essere abilitata al colloquio tramite le porte standard dei seguenti protocolli di comunicazione:
 - HTTP 80 per accedere alle sezioni pubbliche del Portale Web;
 - SMTP/S 465 per spedire messaggi;
 - IMAP/S 993 per ricevere messaggi con client di posta;
 - POP3/S 995 per ricevere messaggi con client di posta.
- Qualora l'utente volesse accedere alla casella PostaCertificat@ utilizzando un client di posta elettronica e per mantenere la riservatezza della comunicazione è necessario che questo venga configurato attivando le impostazioni di sicurezza fornite dal client. In particolare l'utente deve:
 - Impostare i parametri relativi alla sicurezza della connessione su SSL/TLS sia sul server di ingresso che su quello di uscita;
 - attivare i parametri relativi alla autenticazione sicura.
- Nell'utilizzo della casella PostaCertificat@ è necessario custodire la password di accesso con la massima diligenza e non consentirne l'utilizzo a terzi. Si ricorda che la casella PostaCertificat@ del cittadino una volta rilasciata è l'unico indirizzo valido ad ogni effetto giuridico ai fini dei rapporti con le pubbliche amministrazioni e richiedendo la casella avete eletto la casella PostaCertificat@ come l'unico indirizzo per la comunicazione con la PA. In caso di smarrimento, furto o perdita della stessa, si raccomanda di seguire immediatamente le procedure per il reset/cambio della password. In caso di evidenza o sospetto di uso improprio delle casella da parte di terzi a seguito di furto o forzatura della password, si raccomanda di denunciare immediatamente l'accaduto alle autorità competenti
- Per una corretta gestione della propria casella, è buona norma cambiare periodicamente la password, almeno ogni 6 mesi, utilizzando l'apposita funzionalità disponibile sul Portale Web. Accedendo alla casella mediante il portale, il sistema proporrà il cambio password allo scadere di 90 giorni dall'ultimo cambio. Allo scadere di ulteriori 90 giorni, non sarà possibile accedere alla casella senza aver prima provveduto all'aggiornamento della password.
- Si rende inoltre noto che a seguito di tre tentativi di autenticazione falliti l'utenza sarà temporaneamente disabilitata (30 minuti) prima di poter procedere ad una nuova autenticazione.

- In caso di accesso al Portale Web tramite dispositivi sicuri abilitati, si raccomanda di seguire scrupolosamente le indicazioni di sicurezza rilasciate dal soggetto presso il quale è stato acquisito il dispositivo stesso.
- Anche nel caso di caselle PostaCertificat@ per le Pubbliche Amministrazioni, gli utenti abilitati all'accesso, appositamente individuati dalla PA di appartenenza, devono seguire le prassi di sicurezza di cui al presente documento.

Servizio di Assistenza alla Clientela

Per ogni ulteriore informazione in merito all'utilizzo delle caselle PostaCertificat@, si raccomanda di leggere le informazioni presenti sul Portale web www.postacertificata.gov.it o di contattare il Call Center al numero verde gratuito da rete fissa 800.104.464 – da rete mobile il numero 199.135.191 (il costo della chiamata da rete mobile è legato al piano tariffario dell'operatore utilizzato).