

**BancoPosta**

**INFORMAZIONI  
SULLA SICUREZZA  
DEI PAGAMENTI VIA  
INTERNET  
(SERVIZIO BPIOL)**

**Posteitaliane**

# 1. INDICE

<b>1</b>	<b>CARATTERISTICHE DEL SERVIZIO .....</b>	<b>1</b>
<b>2</b>	<b>COME RICHIEDERE L'ATTIVAZIONE DEL SERVIZIO .....</b>	<b>5</b>
<b>3</b>	<b>COME ACCEDERE E CONFIGURARE IL SERVIZIO .....</b>	<b>7</b>
<b>4</b>	<b>COME EFFETTUARE OPERAZIONI DISPOSITIVE E INFORMATIVE .....</b>	<b>11</b>
	4.1 Firma delle operazioni tramite la BPIOL key (Profili Informativo, Monobanca e Multibanca) .....	11
	4.2 Firma tramite APP BPIOL key (Tutti i profili) .....	16
<b>5</b>	<b>FURTO, SMARRIMENTO E UTILIZZO NON AUTORIZZATO DELLE CHIAVI DI ACCESSO, PROCEDURE E RESPONSABILITÀ .....</b>	<b>16</b>
	5.1 Uso non autorizzato o sospetto frodi .....	16
	5.2 Password Amministratore di sistema .....	16
	5.3 BPIOL key (dispositivo fisico, pin e puk) dispositivo mobile e numero cellulare .....	17
<b>6</b>	<b>NON FUNZIONAMENTO O DANNEGGIAMENTO DELLA BPIOL KEY .....</b>	<b>20</b>
<b>7</b>	<b>REGOLE PER LA SICUREZZA .....</b>	<b>21</b>
	7.1 Protezione dei codici e degli strumenti operativi (Password, PIN e PUK della BPIOL KEY) .....	21
	7.2 Ricezione di e-mail sospette (phishing) .....	22
	7.3 Inserimento dei dati personali .....	22
	7.4 Logica di accesso al sito .....	22
	7.5 Aggiornamento di software per la sicurezza informatica .....	23
	7.6 Controllo delle operazioni effettuate .....	23

# 1. CARATTERISTICHE DEL SERVIZIO

BancoPostaImpresa Online (di seguito anche il “Servizio” o “BPIOL”) è il servizio di Remote Banking che Poste Italiane S.p.A. – Patrimonio BancoPosta (di seguito anche “BancoPosta” o “Poste Italiane”) mette a disposizione delle Imprese, delle Associazioni, della Pubblica Amministrazione Centrale e Locale, delle Ditte individuali e dei Liberi Professionisti per accedere ai servizi finanziari del/i proprio/i Conto/i corrente BancoPosta collegandosi direttamente al sito di Poste Italiane [www.poste.it](http://www.poste.it).

Il cliente dovrà dotarsi, a propria cura e spese, di un dispositivo (es. Personal Computer) in grado di stabilire una connessione Internet sicura tramite l'utilizzo di un antivirus ed un “firewall” aggiornati. BancoPosta consiglia di non installare software e di non scaricare file di provenienza sconosciuta poiché potrebbero contenere virus (es. Malware, Trojan, ecc.).

La piattaforma telematica, caratterizzata da elevata sicurezza, consente di gestire online (in funzione del profilo scelto dal cliente), comodamente dal proprio ufficio e in tutta sicurezza, incassi e pagamenti e di conoscerne gli esiti, oltre al saldo e ai movimenti dei propri conti, sia per i rapporti accessi in BancoPosta che per quelli accessi presso altri Operatori Bancari in quanto Poste Italiane è aderente al Consorzio CBI (Customer to Business Interaction).

Gli elementi necessari per l'accesso al servizio da parte **dell'Amministratore di Sistema** sono i seguenti:

- **Codice Azienda** - composto da 10 caratteri; tale codice non può essere modificato;
- **Codice Utente** - attribuito dal Sistema all'atto dell'abilitazione e coincidente per l'Amministratore di Sistema con il Codice Azienda; tale codice non può essere modificato;
- **Password** - composta da almeno 12 caratteri; deve essere modificata dopo il primo accesso e, successivamente, ulteriormente modificata alla scadenza prevista ogni 180 giorni solari. Per gli Utenti Firmatari/Operatori è assegnata dall'Amministratore di Sistema e composta da almeno 8

caratteri, deve essere modificata dagli Utenti Firmatari/Operatori dopo il primo accesso e, successivamente, ulteriormente modificata dagli Utenti Firmatari/Operatori stessi alla scadenza prevista ogni 180 giorni solari.

In conformità alle disposizioni normative che da Settembre 2019 hanno introdotto l'obbligo di adozione della Strong Customer Authentication a 2 (o più) fattori per le operazioni da remoto, per accedere al Servizio ed autorizzare le operazioni dispositive, l'**Amministratore di Sistema** dovrà utilizzare in aggiunta ai Codici e alla Password sopra indicati i seguenti strumenti, in via alternativa e scelti a seconda del profilo del Servizio e della natura giuridica dell'azienda:

- **App BPIOL key**: applicazione da installare sul dispositivo mobile dell'Amministratore di Sistema che, in abbinamento al **Codice di Sicurezza**, consente l'utilizzo del certificato attivo a lui associato per l'autenticazione degli accessi e firma delle configurazioni. Il Codice di Sicurezza (CdS), è il codice alfanumerico scelto dall'Amministratore di sistema al momento dell'attivazione del certificato.
- **BPIOL key**: dispositivo provvisto di Smart Card. Gli elementi che compongono e permettono a loro volta l'utilizzo della BPIOL key per l'accesso al Servizio e firma delle configurazioni sono:
  - **Smart Card**: contenente il Certificato di Firma Digitale<sup>(\*)</sup>; unico per codice fiscale, da richiedere on line al primo accesso;
  - **Token USB**: su cui inserire la Smart Card;
  - **PIN/PUK**: codici numerici per l'uso/sblocco della Smart Card.

(\*) A far data 01/01/2023, ove applicabile, per Firma Digitale può intendersi anche una firma elettronica non qualificata, restando del tutto invariata l'operatività descritta nelle Condizioni Contrattuali del Servizio nonché, per gli scopi ivi previsti, gli effetti dell'apposizione di detta firma.

Analogamente, gli Utenti Firmatari e gli Operatori per poter essere identificati devono digitare negli appositi spazi i 3 codici alfanumerici:

- **Codice Azienda** - composto da 10 caratteri; tale codice non può essere modificato.
- **Codice Utente** - attribuito dal sistema all'atto dell'abilitazione e coincidente con il **Codice Fiscale** dell'Utente Firmatario o dell'Operatore; tale codice non può essere modificato.
- **Password** - assegnata dall'Amministratore di Sistema e composta da almeno 8 caratteri, deve essere modificata dagli Utenti Firmatari/ Operatori dopo il primo accesso e, successivamente, deve essere ulteriormente modificata dagli stessi alla scadenza prevista ogni 180 giorni solari.

Per accedere al Servizio e per la firma delle disposizioni di Incasso e Pagamento, gli Utenti Firmatari e Operatori (gli Operatori solo per l'accesso) devono utilizzare in aggiunta ai Codici e alla Password sopra indicati i seguenti strumenti, in via alternativa, scelti a seconda del profilo del Servizio e della natura giuridica dell'azienda:

- **App BPIOL key**: applicazione da installare sul dispositivo mobile degli Utenti Firmatari e Operatori che, in abbinamento al Codice di Sicurezza, consente l'accesso al certificato attivo a lui associato. Il Codice di Sicurezza (CdS) è il codice alfanumerico da questi scelto al momento dell'attivazione del certificato e installazione dell'App.
- **BPIOL key**, per i soli Utenti Firmatari: dispositivo provvisto di Smart Card. Gli elementi che compongono e permettono a loro volta l'utilizzo della BPIOL key per l'accesso al Servizio e la firma delle disposizioni sono:
  - Smart Card - contenente il *Certificato di Firma Digitale o Elettronica*, unico per codice fiscale, da richiedere on line al primo accesso;
  - Token USB - su cui inserire la Smart Card;
  - PIN/PUK - codici numerici per l'uso/sblocco della Smart Card.
- **BPIOL key light**, per i soli Operatori: dispositivo provvisto di Smart Card. Gli elementi che compongono e permettono a loro volta l'utilizzo della BPIOL key light per l'accesso al Servizio sono:
  - Smart Card - contenente il *certificato elettronico*, unico per codice fiscale, da richiedere tramite l'Amministratore di Sistema;
  - Token USB - su cui inserire la Smart Card;
  - PIN/PUK - codici numerici per l'uso/sblocco della Smart Card.

Tutte le autorizzazioni di Incasso e Pagamento, soggette ad autenticazione forte, devono riportare e collegare alla transazione firmata un insieme di elementi legati alla transazione stessa (es. l'ammontare dell'importo e/o i dati del/i beneficiario/i della stessa), per fornire al cliente garanzia sull'effettivo contenuto ed entità della/e disposizione/i che sta autorizzando.

La validazione delle operazioni, sia singole che massive, avviene sempre tramite l'apposizione del codice PIN della Smart CARD nel caso sia stata scelta la BPIOL Key come strumento di sicurezza o tramite la digitazione, sul device mobile, del Codice di Sicurezza, nel caso sia stata scelta l'App BPIOL key, per i profili standard e i soggetti appartenenti ad aziende con natura giuridica diversa da Libero Professionista, Ditta Individuale o Condomini.

Gli Amministratori e Utenti Firmatari con profilo Easy per l'autorizzazione delle transazioni devono utilizzare obbligatoriamente l'App BPIOL key.

Entrambe le soluzioni garantiscono un elevato standard di sicurezza.

Nel caso in cui le operazioni devono essere autorizzate da più soggetti congiuntamente, è possibile utilizzare sia la BPIOL Key che l'App BPIOL key; tale operatività non è consentita sul profilo EASY.

L'apposizione delle firme congiunte può essere gestita in modalità "sincrona" o "asincrona". Nella modalità asincrona, l'apposizione delle firme con il relativo PIN può avvenire in momenti diversi e non è necessario che i vari soggetti autorizzati a disporre sul conto utilizzino nello stesso istante il medesimo dispositivo connesso ad Internet. Alcune operazioni (ad es. un Postagiorno online) potranno essere effettuate solo in modalità sincrona e, di conseguenza, l'apposizione delle varie firme dovrà necessariamente avvenire nello stesso momento.

Le modalità sopra descritte devono essere applicate, in base alla normativa PSD2, ogni qualvolta il cliente:

- accede online al proprio Conto corrente BancoPosta;
- esegue una transazione di Incasso e Pagamento online;
- esegue una qualsiasi azione nel ruolo di Amministratore di Sistema, attraverso il canale online (configurazione dei dati dell'azienda, Funzioni, Operatori e/o modifica delle precedenti configurazioni).

Il Cliente che abbia attivato il Codice di Sicurezza, mediante l'inserimento di tale codice in App, può autorizzare Operazioni di pagamento disposte direttamente da App oppure impartite dai siti internet di Poste Italiane e/o dai siti/applicazioni per dispositivi di telefonia mobile di esercenti e concluse tramite l'utilizzo delle App. Attraverso l'inserimento del Codice di Sicurezza, il Cliente può consentire anche l'attivazione di un sistema autorizzativo basato sul riconoscimento dei dati biometrici connessi alle impronte digitali (Fingerprint). Tramite l'impiego di tale tecnologia è possibile autorizzare Operazioni di pagamento mediante l'apposizione delle impronte digitali registrate sui sensori del proprio dispositivo mobile (se compatibile con la citata tecnologia). Inoltre, qualora Poste Italiane dovesse rendere disponibile l'autorizzazione di Operazioni di pagamento anche mediante l'utilizzo di ulteriori tecnologie basate sul riconoscimento di altri dati biometrici unici (es. scansione dell'iride, riconoscimento dati fisionomici, riconoscimento facciale, impronta vocale, etc.), il Cliente può fornire la citata autorizzazione anche tramite l'attivazione di tali nuove tecnologie.

## 2. COME RICHIEDERE L'ATTIVAZIONE DEL SERVIZIO

Per attivare il Servizio:

- per chi non è titolare di Conto corrente BancoPosta, è necessario richiedere l'apertura di un Conto corrente BancoPosta e l'attivazione del Servizio sottoscrivendo l'apposita documentazione contrattuale;
- per chi è già titolare di un Conto corrente BancoPosta privo del servizio di Remote Banking, è necessario richiedere l'attivazione del Servizio sottoscrivendo l'apposita documentazione contrattuale.

Il titolare del/dei conto/conti corrente/i BancoPosta è tenuto ad indicare i soggetti autorizzati ad operare e movimentare il/i conto/i attraverso il Servizio ed il soggetto incaricato di gestire le attività connesse alla configurazione ed utilizzo del Servizio stesso (Amministratore di Sistema). I soggetti autorizzati a disporre sul/sui conto/i, nel caso in cui vogliono essere firmatari con delega generale e quindi poter disporre anche tramite i canali fisici di Poste Italiane, devono obbligatoriamente sottoscrivere lo specimen delle firme (Modulo CH7), al momento dell'apertura del Conto corrente BancoPosta o contestualmente alla richiesta di attivazione del Servizio, oltre che compilare l'apposita sezione della documentazione contrattuale messa a disposizione da Poste Italiane.

Nel caso in cui, invece, i soggetti autorizzati vogliono operare sul/sui conto/i solo tramite il Servizio online di BPIOL non devono sottoscrivere lo specimen delle firme (Modulo CH7) ma il "Modulo per l'indicazione dei soggetti abilitati ad operare con deleghe specifiche - BPIOL" dove è necessario indicare anche il tipo di delega e l'operatività a cui vogliono essere abilitati.

Le credenziali di autenticazione dell'Amministratore di Sistema, a prescindere dallo strumento di accesso ed utilizzo scelto, BPIOL key o App BPIOL key, sono inviate al cliente all'indirizzo di posta elettronica/PEC indicato/i nel

modulo di richiesta del Servizio e la password mediante SMS al numero di cellulare appositamente indicato. In fase di primo accesso la password deve essere obbligatoriamente modificata.

La richiesta può essere effettuata in UP in fase di sottoscrizione del servizio BPIOL, ovvero in caso di sostituzione dell'Amministratore di Sistema.

In caso di pratica inviata in lavorazione presso il Back-Office, la comunicazione delle credenziali al cliente, sempre nelle modalità descritte, è differita rispetto alla richiesta ed eseguita una volta completata la lavorazione della pratica.

**Dal 22 settembre 2022 , anche in caso di richiesta di rigenerazione, Poste Italiane non esegue più l'invio delle credenziali di accesso dell'Amministratore di Sistema del servizio BancoPosta Impresa OnLine (BPIOL) tramite busta cartacea.**

La richiesta di rinnovo delle credenziali potrà essere effettuata contattando l'Assistenza Clienti al numero 800.160.000 a condizione che l'Amministratore di Sistema abbia già rilasciato a Poste Italiane un numero di cellulare ancora valido.

Se invece l'Amministratore di Sistema non ha già rilasciato il suo numero di telefono cellulare o deve aggiornare il numero di telefono cellulare, la richiesta può essere eseguita come indicato nel documento pubblicato nella sezione "**Scopri di più**" alla voce "**Guide**" della pagina di accesso al servizio BPIOL.



## 3. COME ACCEDERE E CONFIGURARE IL SERVIZIO

Per utilizzare il Servizio, l'Amministratore di Sistema quando in possesso delle credenziali di primo accesso deve:

- accedere al sito di Poste: [www.poste.it](http://www.poste.it);
- selezionare alla voce "Business" una delle sottosezioni disponibili relative a "Professionisti e piccole Imprese" o "Medie e grandi Imprese" o "Pubblica Amministrazione";
- selezionare la voce "Servizi Finanziari" e successivamente la voce "BancoPostaImpresa Online";
- inserire le credenziali di accesso (codice azienda, codice utente, password);
- scegliere lo strumento di autorizzazione e sicurezza tra quelli disponibili (BPIOL key o App BPIOL key per i profili **Standard** – *Informativo/Monobanca/MultiBanca*); App BPIOL key solo per il profilo **EASY**) nelle modalità previste per il profilo scelto;

Dopo aver effettuato il primo accesso, l'**Amministratore di Sistema** provvede ad effettuare il cambio password ed in seguito, se scelta la BPIOL key come strumento autorizzativo e di sicurezza (alternativa all'App BPIOL key e disponibile per i profili diversi dall'EASY), deve:

- richiedere il proprio kit di firma digitale;
- monitorare lo stato della richiesta attraverso l'apposita funzionalità online:
  - quando in stato "spedito", situazione che evidenzia l'avvenuta spedizione del Kit BPIOL key all'Ufficio Postale scelto, ed una volta ricevuti i codici PIN e PUK, il cliente deve recarsi presso l'UP indicato in fase di richiesta online del certificato e ritirare la propria BPIOL key (il dispositivo token USB con a bordo la Smart Card ed il certificato di firma digitale) e consegnare le condizioni contrattuali scaricate dal sito e sottoscritte con la Certification Authority per il servizio di firma digitale;
- accedere al Servizio online ed entrare nell'apposita sezione dedicata per:
  - eseguire la configurazione ed abilitazione degli ulteriori soggetti che

devono operare sul sito, per effettuare operazioni informative e/o dispositive (Utenti Firmatari), o dei soggetti autorizzati ad effettuare solo operazioni informative e predisporre disposizioni/ flussi senza la possibilità di poterli autorizzare (Operatori);


- generare le credenziali di accesso per ciascun Utente Firmatario e/o Operatore ed abilitarli all'utilizzo del Servizio apponendo la propria firma digitale;
- comunicare le credenziali di accesso a ciascun Utente Firmatario ed Operatore.

Una volta abilitati dall'Amministratore di Sistema, gli Utenti Firmatari e gli Operatori di profili Standard devono cambiare anch'essi la propria password; al primo accesso al sistema, anche gli Utenti Firmatari possono scegliere e richiedere quindi a loro volta il proprio certificato di Firma Digitale, con annessa BPIOL key, o in alternativa l'App BPIOL key, con le stesse modalità previste per l'Amministratore di Sistema. Ricordiamo che sul profilo EASY è disponibile solo l'App BPIOL key.

**N.B.:** per quanto riguarda gli Operatori, è l'Amministratore di Sistema che provvede necessariamente in prima istanza alla prima richiesta per loro conto dei dispositivi, scegliendo sempre tra la BPIOL key light (profili diversi da EASY ) e l'App BPIOL key, curandosi di effettuare la consegna al diretto interessato nel primo caso, una volta ricevuto il dispositivo presso l'indirizzo dell'azienda comunicato in fase di richiesta; ovvero in alternativa associando l>ID App dell'Operatore nell'apposita procedura disponibile sul sito online al termine dell'installazione nel secondo caso.

La BPIOL key, qualora scelta come strumento di autorizzazione può essere utilizzata dall'Amministratore di Sistema, per eseguire tutte le operazioni di configurazione ed abilitazione online, nonché utilizzata dagli Utenti Firmatari per eseguire operazioni dispositive a valere sul/sui conto/i devono utilizzare la BPIOL Key. Lo strumento è un dispositivo USB contenente una Smart card con certificato di firma digitale qualificata per la firma delle disposizioni intestato al titolare richiedente. Analogamente, la BPIOL key light è parimenti uno strumento della stessa tipologia ma utilizzata unicamente dagli Operatori nella fase di accesso e dotata differentemente di un certificato elettronico di autenticazione.



La richiesta del Kit BPIOL key può essere effettuata dall'Amministratore, o dagli Utenti Firmatari, esclusivamente on line dalla sezione "GESTIONE SICUREZZA" accessibile dall'icona  presente in alto a dx e selezionando nella combobox la funzione "**Richiesta BPIOL key**". È consentito l'inserimento di **una sola richiesta per Codice Fiscale** che può essere monitorata online nell'avanzamento della lavorazione (stato certificato **Richiesto/Inviato/In carico/Emesso/Spedito**).

In caso di **Liberi Professionisti, Ditte Individuali e Condomini** di appartenenza al profilo EASY, l'Amministratore di Sistema e gli Utenti Firmatari in fase di sottoscrizione del servizio BPIOL dovranno dotarsi obbligatoriamente dell'App BPIOL key, quale strumento di accesso e utilizzo del Servizio, per il tramite dei canali fisici di Poste Italiane (Uffici Postali e/o account commerciali).

**N.B.:** da giugno 2022 per dismissione del servizio, l'Amministratore di Sistema e gli Utenti Firmatari di un profilo EASY anche se già in possesso del numero cellulare certificato, **non** potranno più procedere autonomamente ad associare l'App BPIOL key, quindi dotarsi dello strumento, utilizzando la modalità Web messa a disposizione online mediante l'apposizione del codice OTP ricevuto sul numero di cellulare certificato via SMS, ma dovrà recarsi necessariamente in Ufficio Postale o ricorrere all' account commerciale per l'associazione dell'App.

L'Amministratore di Sistema, gli Utenti Firmatari e Operatori che hanno scelto l'App BPIOL key come strumento di sicurezza, obbligatoria per i primi due soggetti sul profilo EASY, al primo accesso, dopo aver modificato la password di primo accesso, devono completare l'attivazione dell'App

BPIOL key inquadrando con il dispositivo mobile su cui è installata l'App stessa il QR CODE visualizzato sul canale WEB BPIOL, definendo nell'App il suo Codice di Sicurezza, attivando e associando il certificato elettronico al proprio dispositivo mobile.

Da tale momento, analogamente a quanto descritto per i dispositivi BPIOL key, l'App BPIOL key sarà necessaria per l'Amministratore di Sistema per gestire l'abilitazione online degli Utenti Firmatari e Operatori creandone le rispettive credenziali.

Nei casi descritti, qualora l'Amministratore di Sistema o l'Utente Firmatario, sia già in possesso di una BPIOL key con Certificato di Firma Digitale attivo, per profili diversi dall'EASY, può dotarsi autonomamente dell'App BPIOL key senza necessità di recarsi in Ufficio Postale e/o ricorrere all'account commerciale, utilizzando le modalità web messe a disposizione da Poste Italiane e firmando la richiesta con la BPIOL key in suo possesso.

Successivamente all'attivazione dell'App BPIOL key, il Certificato di Firma Digitale non potrà essere più utilizzato quale strumento di accesso ed utilizzo del Servizio.

Nel caso in cui la stessa persona ricopra il ruolo di Amministratore di Sistema e Utente Firmatario, indipendentemente dal fatto che abbia scelto l'App BPIOL key o la BPIOL key, deve utilizzare tale strumento sia per l'accesso che per le funzioni di gestione del Servizio e firma delle operazioni dispositive.

I flussi elettronici delle disposizioni, predisposti secondo gli standard stabiliti da Poste Italiane e dal CBI, dovranno essere autorizzati tramite la BPIOL key o l'App BPIOL key.

Gli Amministratori di Sistema e gli Utenti Firmatari che operano per più aziende potranno utilizzare la stessa BPIOL key o App BPIOL key per utilizzare il Servizio in nome e per conto di tutte le aziende dalle quali sono autorizzati ad utilizzare il Servizio stesso.

## 4. COME EFFETTUARE OPERAZIONI DISPOSITIVE E INFORMATIVE

Dopo aver eseguito l'accesso al Servizio come descritto nel paragrafo 3, dalla sezione dedicata ai Servizi Informativi di BPIOL è possibile visualizzare ed eventualmente scaricare in locale sul proprio PC le rendicontazioni giornaliere relative ai saldi e ai movimenti di conti correnti BancoPosta e, all'interno della sezione di menù relativa allo specifico prodotto, gli esiti delle operazioni dispositive (ad es. gli esiti dei bonifici).

L'Amministratore di Sistema e gli Utenti Firmatari potranno effettuare la gestione delle autorizzazioni delle operazioni del Servizio utilizzando unicamente la BPIOL key o l'App BPIOL key.

### 4.1 Firma delle operazioni tramite la BPIOL key (Profili Informativo, Monobanca e Multibanca)

Per procedere con la firma, è necessario inserire la BPIOL key nell'apposita porta USB del PC al fine di identificare il dispositivo e caricare il certificato di firma digitale. Per autorizzare la disposizione è necessario inserire il codice PIN ricevuto nella fase di richiesta del certificato.

L'errato inserimento del codice PIN, per 6 volte consecutive, genera il blocco della Smart Card. Lo sblocco è consentito tramite l'apposita funzione della BPIOL key che richiede l'inserimento del codice PUK (ricevuto unitamente al codice PIN), secondo le modalità indicate nel Manuale Operativo della BPIOL key presente all'interno della sezione relativa alla BPIOL Key in Funzioni Generali - Assistenza.

Entrambi i codici PIN e PUK sono forniti dalla Certification Authority di Poste Italiane, non sono modificabili dall'Utente Firmatario e, come la Smart Card, sono da considerarsi strettamente personali. La modalità di autorizzazione

delle operazioni dispositive tramite firma digitale permette l'autenticazione dell'Utente Firmatario, garantisce l'integrità del flusso e la non ripudiabilità dell'operazione una volta firmata ed eseguita.

## FIRMA SINGOLA

Dal momento della selezione del flusso di disposizioni, selezionando il pulsante "Crea Flusso" si visualizza la pagina di apposizione della firma. Inserendo la BPIOL key nella porta USB del computer e selezionando il tasto "Ricarica Dispositivi" è visualizzato e già preselezionato il certificato presente nel dispositivo.

Successivamente, è necessario inserire il PIN del certificato di firma digitale selezionato e cliccare sul pulsante "Apponi Firma", per apporre la firma sul flusso. Quando nel box Firme Apposte è visualizzato il Codice Fiscale del titolare della firma già apposta, selezionare il pulsante "Salva Firma" per memorizzare la firma e spedire il flusso successivamente, oppure il pulsante "Spedisci" per spedire il flusso. La figura successiva presenta la pagina di accesso alle funzioni di verifica della spedizione.

<input type="checkbox"/>		13/06/19 15:25:51	Richiami Bonifici Domiciliati	aaaa	07601	681	13/06/19	496,00	10	Da firmare	-	-	-	13/06/19 15:25:51	In linea	10.15.36.108
<input type="checkbox"/>		13/06/19 14:27:33	Bonifici XML	XPCI427303	07601	156042885149300LRW2K	13/06/19	86.690,53	11	In carico banca	BNGPNC80P43H5010		13/06/19 14:42:18	13/06/19 14:42:51	In linea	10.15.36.108
<input type="checkbox"/>		12/06/19 12:26:43	Bonifici XML	XPCI226402	07601	156033520147100FQW2K	11/06/19	86.690,53	11	In carico banca	BNGPNC80P43H5010		12/06/19 12:28:28	12/06/19 12:28:51	In linea	10.15.36.108
<input type="checkbox"/>		11/06/19 15:58:21	Bonifici Domiciliati	aa	07601	8718	11/06/19	55,00	1	Da firmare	-	-	-	11/06/19 15:58:21	In linea	10.17.157.54
<input type="checkbox"/>		11/06/19 15:53:46	Bonifici Domiciliati	12	07601	8717	11/06/19	12,00	1	Da firmare	-	-	-	11/06/19 15:53:46	In linea	10.15.46.148

Pagina 1/ 23 >

## FIRMA CONGIUNTA

In caso di firma congiunta, è possibile firmare utilizzando le BPIOL key dei rispettivi Utenti Firmatari. La modalità prevede l'apposizione di una prima firma attraverso uno dei due dispositivi, esattamente come nel caso di firma singola, e selezionando il pulsante "Salva Firma".

Il secondo Utente Firmatario, nella medesima sessione (obbligatorio per le operazioni in tempo reale, come ad es. Postagiuro on line) o anche accedendo al Servizio BPIOL successivamente da altra postazione, visualizza il Codice

Fiscale del primo Utente Firmatario e ripete l'operazione di "Ricarica Dispositivi" e "Apponi Firma" per l'apposizione della seconda firma. Selezionare, infine, il pulsante "Spedisci" per spedire il flusso e accedere alla pagina di esito dell'operazione contenente i link per la verifica dell'esito della spedizione.

Solo dopo aver eseguito i passi necessari per autorizzare un'operazione dispositiva, essa si intende eseguita e non più revocabile.

L'Utente Firmatario, può visualizzare ed eventualmente scaricare sul proprio computer i dati relativi alle movimentazioni operati sui propri conti correnti accessi anche presso altri istituti (in caso di profilo MultiBanca) e con cui opera quotidianamente, tra cui: le rendicontazioni giornaliere relative ai saldi e ai movimenti dei suoi conti correnti ordinari, dei rapporti di portafoglio e dei dossier titoli; l'esito delle operazioni dispositive, quali gli esiti dei bonifici, le rendicontazioni degli incassi, le quietanze delle deleghe F24, e molto altro ancora. Le conferme di avvenuta esecuzione delle operazioni dispositive devono essere sempre controllate; è importante verificare che siano state addebitate solo le operazioni effettuate.

## 4.2 Firma tramite APP Bpiol key (Tutti i profili)

A far data dal 12 settembre 2019, se scelta come modalità di accesso e firma dagli Amministratori di Sistema e dagli Utenti Firmatari per i profili Standard, obbligatoria per l'accesso e firma delle disposizioni del profilo Easy per Ditte individuali, Liberi Professionisti e Condomini, è possibile disporre di tre diverse modalità di firma delle disposizioni mediante l'App BPIOL key: **online**, **offline**, **in mobilità**.

### **Firma con App in modalità online**

L'Operatore/Utente Firmatario inserisce una nuova disposizione/flusso, oppure ne seleziona una esistente da firmare: selezionando il pulsante "Firmo Io", il sistema invia una notifica all'App dell'Utente Firmatario con i dati dell'operazione e le informazioni addizionali e di sicurezza necessarie; viene bloccata contestualmente la sessione Web con un popup che avverte l'Utente Firmatario di utilizzare il dispositivo mobile per completare l'operazione; l'Utente Firmatario tocca la notifica ricevuta che apre a sua volta l'App (oppure la apre direttamente).

In questo scenario è possibile a questo punto per l'Utente Firmatario, sempre in App:

- inserire il Codice di Sicurezza per entrare nell'APP;
- visualizzare i dati dell'operazione che deve autorizzare;
- digitare eventuali dati aggiuntivi che gli sono richiesti per garantire che abbia contezza di cosa sta autorizzando;
- fornire la password del Servizio BPIOL, se l'importo è tale da rientrare nella casistica che prevede un incremento della sicurezza;
- inserire nuovamente il Codice di Sicurezza per conferma finale.

L'App, a questo punto, provvede a inviare la risposta che se elaborata positivamente autorizza la disposizione/flusso.

### **Firma con App in modalità offline**

L'Operatore/Utente Firmatario inserisce una nuova disposizione/flusso oppure ne seleziona una esistente da firmare; premendo il pulsante "Firmo lo senza connessione", il sistema visualizza, sulla pagina Web un QR-Code interpretabile solo dall'App dell'Utente Firmatario (il QR-Code contiene i dati dell'operazione e le informazioni aggiuntive e di sicurezza necessarie); l'Utente Firmatario apre autonomamente la sua App e sempre tramite essa:

- scansiona il QR-Code e visualizza i dati dell'operazione che deve autorizzare;
- inserisce eventuali dati aggiuntivi che gli sono richiesti per garantire che abbia contezza di cosa sta autorizzando;
- inserisce la password del Servizio BPIOL, se l'importo è tale da rientrare nella casistica che prevede un incremento della sicurezza.

L'App, a questo punto, visualizza una stringa alfanumerica e l'Utente Firmatario tornando alla pagina WEB:

- inserisce la stringa alfanumerica visualizzata dall'App in un apposito campo presente sulla pagina;
- digita il Codice di Sicurezza in un apposito campo presente sulla pagina.

L'App provvede a inviare la risposta (i.e. la stringa alfanumerica inserita e il Codice di Sicurezza) che se elaborata positivamente autorizza la disposizione/flusso.



### **Firma con App in mobilità**

L'Operatore inserisce una nuova disposizione/flusso, oppure ne seleziona una esistente da firmare, e preme il pulsante "Firma di altro Operatore in mobilità".

L'Operatore seleziona un Firmatario da una lista visualizzata dalla pagina Web e, in questo caso, il sistema invia una notifica all'App del Firmatario con i dati dell'Operazione e le informazioni addizionali e di sicurezza necessarie; contestualmente, viene bloccata la sessione Web con un popup che avverte lo stesso Operatore di aver inviato la richiesta di autorizzazione sul dispositivo del Firmatario selezionato e di essere in attesa di risposta per completare l'operazione.

L'Utente Firmatario tocca la notifica ricevuta, che apre l'App (oppure la apre direttamente) e, sempre in App:

- inserisce il Codice di Sicurezza per entrare nell'App;
- visualizza i dati dell'operazione che deve autorizzare;
- digita eventuali dati addizionali che gli sono richiesti per garantire che abbia contezza di cosa sta autorizzando;
- fornisce la password del Servizio BPIOL (questo passaggio è sempre necessario essendo utente diverso da quello che ha richiesto la firma della disposizione);
- inserisce nuovamente il Codice di Sicurezza.

L'App provvede a inviare la risposta che se elaborata positivamente autorizza la disposizione/flusso.

## 5. FURTO O SMARRIMENTO E UTILIZZO NON AUTORIZZATO DELLE CHIAVI DI ACCESSO E UTILIZZO DEL SERVIZIO: PROCEDURE DA SEGUIRE E RESPONSABILITÀ

In caso di smarrimento o furto, nonché di uso non autorizzato o sospetto degli strumenti identificativi (Codice Azienda, Codice Utente e Password) e operativi: BPIOL key, PIN e PUK della BPIOL key, BPIOL key light, PIN e PUK della BPIOL key light, l'App BPIOL key e il Codice di Sicurezza dell'App ) il Cliente è tenuto a comunicare immediatamente l'accaduto a Poste Italiane, con le modalità di seguito indicate non appena ne viene a conoscenza ed altresì a sporgere tempestivamente, esclusivamente nei casi di furto e/o smarrimento dei suddetti strumenti, denuncia alle Autorità competenti.

16

### 5.1 USO NON AUTORIZZATO O SOSPETTO FRODE

In caso di abuso riscontrato o sospetto (frodi) il Cliente deve contattare il **numero verde dell'Assistenza 800.160.000** per le opportune azioni di contrasto. Successivi ed eventuali aggiornamenti alla numerazione saranno disponibili sul sito [www.poste.it](http://www.poste.it) nella sezione "**Chiamaci**" del servizio di Assistenza.

### 5.2 PASSWORD AMMINISTRATORE DI SISTEMA

Per richiedere una nuova password di Amministratore di Sistema il Cliente dovrà contattare il **numero verde dell'Assistenza 800.160.000**. Successivi ed eventuali aggiornamenti alla numerazione saranno disponibili sul sito [www.poste.it](http://www.poste.it) nella sezione "**Chiamaci**" del servizio di Assistenza. L'Operatore di Assistenza dopo aver effettuato il riconoscimento provvede ad inviare una nuova Password, da modificare dopo il primo accesso, con un nuovo sms sul cellulare rilasciato.

## 5.3 BPIOL KEY (DISPOSITIVO FISICO, PIN E PUK) DISPOSITIVO MOBILE E NUMERO CELLULARE

Se il furto o lo smarrimento, o l'uso non autorizzato o sospetto, riguarda la BPIOL key, il cliente potrà richiedere l'immediata sospensione del relativo certificato di firma digitale dal Servizio BPIOL seguendo la procedura guidata:

Posteitaliane

Operator: LMTGDU7BPOH4501A Azienda: 0007050320 - prova1 Codice SIA: SAFER Codice CLIC: SIA SAFER

SERVIZI INFORMATIVI GESTIONE LIQUIDITA' PAGAMENTI INCASSI BOLLETTINI CARTE

Firma digitale Esporta movimenti Esporta esiti pagamenti Esporta esiti incassi Esporta flussi bollettini Esporta flussi carte Gestione dati Istruzioni operative

Funzioni generali > Firma digitale > Gestione bpiol key > Sospensione > Revoca > Riattivazione Sospensione/Revoca/Riattivazione

Il certificato di firma digitale della BPIOL key può essere sospeso con effetto immediato\* in caso di smarrimento o furto o comunque in tutti i casi in cui la sicurezza di tale certificato non è più certa. La sospensione può anche essere differita\*\* ad una data successiva a quella della richiesta.

La validità del certificato di firma digitale della BPIOL key può essere revocata su richiesta del cliente (ad esempio nel caso di blocco del codice PUK) in seguito alla revoca\*\* il certificato di firma digitale non può essere riattivato. Il cliente può richiedere l'emissione di un nuovo certificato di firma digitale tramite la funzione "Firma digitale/Richiesta BPIOL key".

In seguito alla sospensione immediata o differita, il certificato di firma digitale è sospeso fino alla naturale scadenza dello stesso. Si può richiedere la riattivazione\*\* nel caso in cui si desideri utilizzare il medesimo certificato.

\*Per richiedere la sospensione immediata tramite la procedura online è necessario avere a disposizione il codice univoco ed il codice di sospensione immediata ricevuti in occasione dell'emissione della BPIOL key.  
Nel caso di dimenticanza dei codici telefonare al Servizio Clienti BancoPostasponde al numero gratuito 800 00 33 22 (opzione 2 oppure 3) dalle 8.00 alle 20.00 dal lunedì al sabato.  
\*\*Per richiedere la sospensione differita, la revoca o la riattivazione occorre inviare, via fax o email a Postecert, il "Modulo per la richiesta di Sospensione, Revoca e/o Riattivazione del certificato qualificato" allegando copia del codice fiscale e del documento di identità. Per precampiare il suddetto Modulo basta eseguire le rispettive funzionalità online.

Come riportato nella figura sopra, in caso di dimenticanza oppure furto, smarrimento, nonché uso non autorizzato o sospetto anche dei codici di sospensione il Cliente può telefonare al **numero verde dell'Assistenza 800.160.000**. Successivi ed eventuali aggiornamenti alla numerazione saranno disponibili sul sito [www.poste.it](http://www.poste.it) nella sezione **"Chiamaci"** del servizio di Assistenza. Nell'ambito delle funzioni disponibili per il funzionamento e utilizzo della BPIOL key, il Cliente può richiedere, oltre alla sospensione immediata del certificato, anche la:

- **Sospensione differita** con effetto a partire da una data specifica;
- **Revoca** (ad es. per blocco del codice PUK, il certificato di firma digitale non può essere riattivato ed il cliente deve richiedere l'emissione di uno nuovo; disponibile anche per la BPIOL key light);
- **Riattivazione** (nel caso si voglia riutilizzare il certificato, che era stato sospeso in modalità immediata o differita, fino alla sua naturale scadenza).

Il certificato di firma digitale della BPIOL key scade dopo 3 anni dall'attivazione dello stesso, e può essere rinnovato per altri anni, purché il rinnovo avvenga prima della scadenza. La procedura di rinnovo deve essere effettuata online e può essere eseguita solo nel periodo compreso tra 60 giorni solari precedenti la scadenza del certificato e la scadenza stessa.

Il rinnovo può essere fatto due volte prorogando la validità del certificato di 6 anni rispetto al primo periodo di validità di 3 anni. Se il certificato non è rinnovato entro la prima scadenza oppure trascorsi tre anni dal rinnovo, deve essere necessariamente richiesto un nuovo certificato, direttamente dal Servizio BPIOL, attraverso la procedura disponibile online.

In caso di furto o smarrimento del dispositivo mobile o del Codice di Sicurezza, è necessario richiedere immediatamente il blocco dell'App contattando il **numero verde dell'Assistenza 800.160.000**. Successivi ed eventuali aggiornamenti alla numerazione saranno disponibili sul sito [www.poste.it](http://www.poste.it) nella sezione "**Chiamaci**" del servizio di Assistenza.

Il Cliente non sopporta alcuna perdita derivante dall'utilizzo degli strumenti identificativi ed operativi smarriti, sottratti o utilizzati indebitamente, salvo il caso in cui abbia agito in modo fraudolento, qualora: a) lo smarrimento, la sottrazione o l'appropriazione indebita degli strumenti non potevano essere notati dal Cliente stesso prima di un pagamento o se la perdita è stata causata da atti o omissioni di dipendenti, agenti o succursali di Poste Italiane o dell'eventuale ente cui Poste Italiane abbia esternalizzato le attività; b) l'utilizzo degli strumenti sia successivo alla comunicazione di blocco; c) Poste Italiane non abbia adempiuto all'obbligo di assicurare al Cliente di eseguire efficacemente e a titolo gratuito la comunicazione di blocco.

Negli altri casi, il Cliente sopporta, per un importo complessivamente non superiore a 50 (cinquanta) euro, la perdita relativa a operazioni di pagamento non autorizzate derivante dall'utilizzo indebito degli strumenti conseguente al loro furto o smarrimento o appropriazione indebita, salvo il caso in cui abbia agito in modo fraudolento o non abbia adempiuto, con dolo o colpa grave, a uno o più obblighi disciplinati dalle condizioni contrattuali (utilizzo degli strumenti e comunicazione dell'eventuale loro furto, smarrimento, uso non autorizzato), dove non si applica il limite del citato importo.

Poste Italiane assicura che: (i) i codici e gli strumenti operativi consentono l'utilizzo del Servizio in modo protetto, garantendo elevati standard di sicurezza; (ii) i codici e gli strumenti operativi e i dati relativi alle operazioni eseguite non siano accessibili a soggetti diversi dal Cliente; (iii) il Cliente sia sempre nella condizione di eseguire la comunicazione avente ad oggetto il furto, lo smarrimento, l'uso non autorizzato o sospetto dei codici e degli strumenti operativi.

Poste Italiane tutela costantemente i dati dei suoi clienti attraverso l'adozione dei più moderni sistemi di sicurezza e fornisce tutte le informazioni utili per usufruire in modo sicuro dei servizi di pagamento via Internet. Per ulteriori dettagli è disponibile apposito materiale informativo sul sito [www.poste.it](http://www.poste.it).

Le modalità di scadenza e rinnovo del certificato elettronico si applicano anche alla BPIOL key light. Sarà possibile, inoltre, utilizzare le stesse procedure e le stesse modalità online per la richiesta di revoca del certificato elettronico della BPIOL key light e procedere quindi, per il tramite del proprio Amministratore di Sistema, alla richiesta online di un nuovo dispositivo nelle stesse modalità di prima emissione, nonché delle procedure di blocco dell'App BPIOL key, per quest'ultima contattando il **numero verde dell'Assistenza 800.160.000**. Successivi ed eventuali aggiornamenti alla numerazione saranno disponibili sul sito [www.poste.it](http://www.poste.it) nella sezione **"Chiamaci"** del servizio di Assistenza.

## 6. NON FUNZIONAMENTO O DANNEGGIAMENTO DELLA BPIOL KEY

Nel caso di non funzionamento o danneggiamento della BPIOL Key o BPIOL key light, il Cliente può richiederne la sostituzione presso l'Ufficio Postale di riferimento del Conto o al proprio account commerciale. In questi casi il Cliente dovrà compilare l'apposito modulo e riconsegnare il kit di firma in suo possesso e si procederà alla revoca dello stesso a alla richiesta di un nuovo certificato.

## 7. REGOLE PER LA SICUREZZA

Di seguito, alcune semplici regole da seguire per accedere al Servizio BPIOL (BancoPostalImpresa Online) con la massima sicurezza.

### 7.1 PROTEZIONE DEI CODICI E DEGLI STRUMENTI OPERATIVI (PASSWORD, PIN E PUK DELLA BPIOL KEY)

I codici sono strettamente personali e pertanto devono essere custoditi dal Cliente con la massima cura, mai comunicati ad altri adottando misure idonee a garantire la sicurezza e riservatezza. È preferibile non conservare i codici insieme, né annotarli su unico documento.

Per una maggiore sicurezza si consiglia di modificare periodicamente le Password. Il sistema impone comunque un cambio della password obbligatorio ogni 180 giorni.

È consigliato utilizzare una Password con le seguenti caratteristiche:

- lunghezza minima: 12 caratteri per l'Amministratore di Sistema e 8 caratteri per Firmatari e Operatori;
- che contenga almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale (è obbligatorio almeno un carattere speciale);
- che non corrisponda o contenga riferimenti a dati personali (ad es. indirizzo, telefono, codice fiscale, numero della patente, nomi propri, date di nascita, ecc.) o agevolmente riconducibili all'utente;
- che non sia uguale alle Password precedenti.

È importante, non utilizzare la stessa Password utilizzata per accedere ad altri siti web.

## 7.2 RICEZIONE DI E-MAIL SOSPETTE (PHISHING)

L'accesso al servizio BPIOL BancoPostalImpresa Online deve essere effettuato partendo dall'indirizzo Web "[www.poste.it](http://www.poste.it)" o dall'indirizzo "<https://bancopostaimpresaonline.poste.it/bpiol1/>", evitando di accedere da link presenti all'interno di email "sospette". Poste Italiane, direttamente o tramite terzi, non richiede mai ai propri clienti, attraverso messaggi di posta elettronica, telefonate o lettere, di fornire i codici di accesso personali quali il Codice Utente, la Password, il PIN o il PUK BPIOL key o, il PIN o il PUK BPIOL key light e Codice di Sicurezza App.

## 7.3 INSERIMENTO DEI DATI PERSONALI

Diffidare di improvvisi cambiamenti nella modalità con cui viene chiesto di inserire i codici di accesso a BancoPosta Impresa Online: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite pop-up (una finestra aggiuntiva di dimensioni ridotte) e in tutti i casi in cui viene richiesto di utilizzare modalità diverse da quelle indicate nelle presenti istruzioni operative.

In questi casi, contattare immediatamente Poste Italiane chiamando il **numero verde numero verde dell'Assistenza 800.160.000** oppure inviando un'e-mail a [info@poste.it](mailto:info@poste.it). Successivi ed eventuali aggiornamenti alla numerazione saranno disponibili sul sito [www.poste.it](http://www.poste.it) nella sezione "**Chiamaci**" del servizio di Assistenza.

## 7.4 LOGICA DI ACCESSO AL SITO

L'accesso al sito deve avvenire digitando l'indirizzo [www.poste.it](http://www.poste.it) o l'indirizzo <https://bancopostaimpresaonline.poste.it/bpiol1/> direttamente nel browser Internet.

Poste Italiane è costantemente impegnata a tutelare i dati dei suoi clienti attraverso l'adozione dei più moderni sistemi di sicurezza. Questi sistemi garantiscono comunicazioni affidabili e sicure attraverso l'adozione del protocollo Https.

È quindi importante che durante l'inserimento dei dati riservati nella pagina web, ci si assicuri che si tratti di una pagina protetta. Le pagine protette



sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://".

Inoltre, le pagine protette contengono un lucchetto nella parte in alto a sinistra della barra degli indirizzi del browser.

Cliccando due volte sul lucchetto, è possibile verificare l'esistenza di un "certificato" che garantisce l'autenticità del sito.

È importante controllare a chi (e da chi) è stato rilasciato il certificato; in questo caso, deve risultare che il certificato sia rilasciato da Poste Italiane S.p.A..

## **7.5 AGGIORNAMENTO DI SOFTWARE PER LA SICUREZZA INFORMATICA**

Il sistema operativo e i programmi di protezione del computer (antivirus, antispyware, ecc.) devono essere costantemente aggiornati. Le aziende produttrici dei software rendono periodicamente disponibili online (e scaricabili gratuitamente) aggiornamenti (cosiddette "patch") che incrementano la sicurezza del sistema operativo e del browser. Sui siti di queste aziende è anche possibile verificare che il proprio browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le "patch".

## **7.6 CONTROLLO DELLE OPERAZIONI EFFETTUATE**

Gli estratti conto e le conferme di avvenuto pagamento devono essere sempre controllate; è importante verificare che siano state addebitate solo le operazioni effettuate. La data e l'ora dell'ultimo accesso, presenti nella pagina di benvenuto del Servizio BPIOL BancoPostaImpresa Online, rappresentano un valido strumento di controllo.

## Come possiamo aiutarti?



### Contattaci

Vai su **poste.it** nella sezione Assistenza e compila il modulo



### Chiamaci

**800.160.000**

numero gratuito, attivo dal lunedì al sabato (dalle 8.00 alle 20.00, escluso i festivi)



**Posteitaliane**