

# **Agenzi@Bpb *AZIENDE***

---

## **Guida all'utilizzo del *TOKEN FISICO***

## PREMESSA

La nuova "**Direttiva Europea sui Servizi di Pagamento**" (c.d. PSD2) ha ridefinito gli standard di sicurezza per i clienti che operano attraverso i propri conti accessibili online adottando l'**Autenticazione Forte** (meglio nota come "*Strong Customer Authentication*" o SCA).

L'Autenticazione forte è un sistema di sicurezza che garantisce l'identificazione e l'autenticazione univoca quando il cliente:

- accede al suo conto di pagamento disponibile online;
- dispone un'operazione di pagamento utilizzando conti di pagamento disponibili online; utilizzando sia i canali telematici della Banca sia le soluzioni offerte dalle Terze Parti autorizzate.

Per incrementare ulteriormente la sicurezza e la protezione dei clienti che operano online, la Direttiva ha anche introdotto il requisito del "**Collegamento dinamico**" (meglio noto come DynamicLinking) ovvero un codice di autenticazione collegato in modo univoco all'operazione da disporre e che prende in considerazione gli elementi fondamentali del pagamento (es. importo e credenziali del beneficiario).

In piena applicazione della Direttiva e nell'ottica di garantire la sicurezza dei propri clienti, Banca Popolare di Bari mette a disposizione dei propri clienti Azienda il nuovo token Fisico Vasco DP270.

Il rilascio è gratuito solo in occasione dell'adeguamento normativo sia per le utenze master che per le utenze secondarie. Per le nuove accensioni sarà applicato il costo previsto dalle disposizioni di trasparenza.

**NOTA BENE:** Ti ricordiamo che a partire dal 14 settembre 2019, se non avrai provveduto a sostituire il tuo dispositivo di autenticazione con una delle soluzioni messe a disposizione dalla Banca alla propria clientela, non potrai più accedere ed operare tramite la piattaforma **agenzi@bpb Aziende**.

In questa guida parliamo delle nuove modalità di utilizzo del **Token Fisico**.

## IL TOKEN FISICO

Il Token Fisico è un dispositivo personale di sicurezza, costituito da un display e da vari pulsanti, che produce codici numerici monouso (One Time Password – OTP) e che il cliente utilizza sulla propria piattaforma di agenzi@bpb Aziende per autenticarsi e per autorizzare le operazioni di pagamento.

È protetto da un PIN a 4 cifre scelto dall'utente alla prima accensione.

Il token deve essere utilizzato su agenzi@bpb nelle fasi di:

- accesso (login);
- autorizzazione delle disposizioni di pagamento.

**Per ricevere il token fisico devi recarti in Filiale e richiederne la consegna dal momento che il dispositivo deve essere associato al tuo contratto di servizi telematici.**

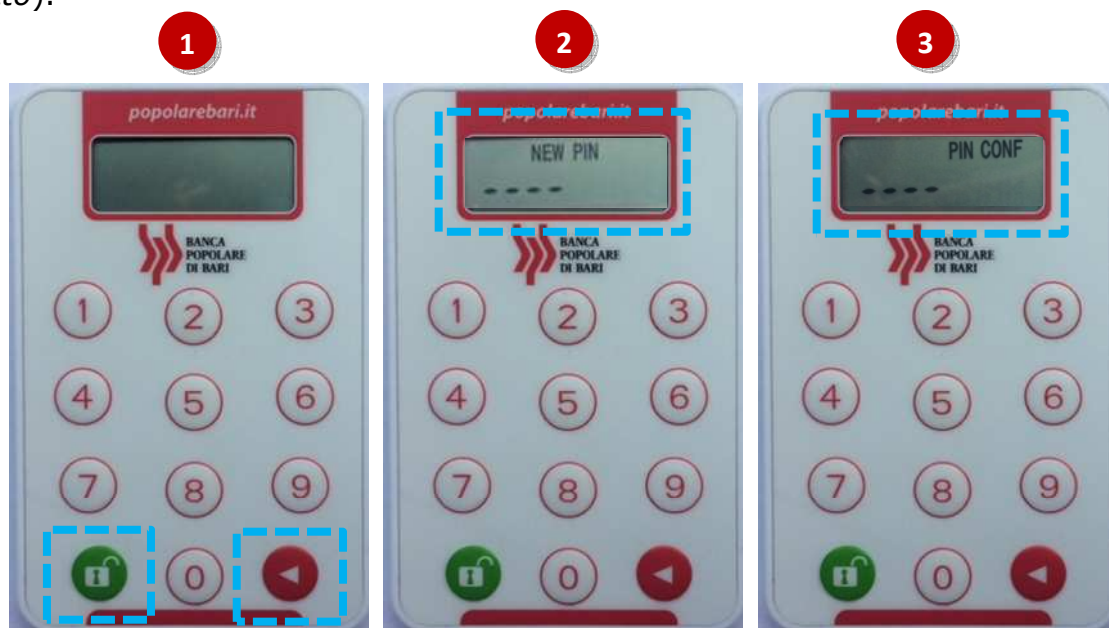
**Anche i token fisici delle utenze secondarie devono essere ritirati in Filiale dal titolare del contratto telematico.**

Di seguito trovi le istruzioni per utilizzare il token fisico con **agenzi@bpb Aziende**.

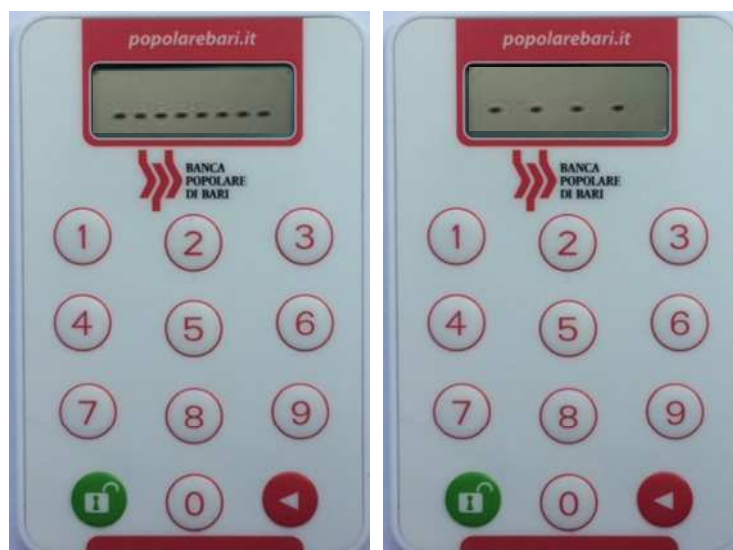
## GENERAZIONE PIN

Il Token Fisico è protetto da un PIN di 4 cifre scelto dall'utente in fase di prima accensione. Per configurare il PIN devi seguire le istruzioni di seguito riportate:

1. Per attivare il dispositivo, **tieni premuto il tasto rosso e poi contemporaneamente premi il tasto verde** sino a quando non si attiva sul display l'indicazione **"New PIN"** (vedi immagine 1 sotto);
2. A seguito della prima attivazione il dispositivo richiede l'attivazione del PIN, codice personale a 4 cifre a scelta del cliente. **Digita il PIN sul tastierino** (vedi immagine 2 sotto);
3. **Conferma il PIN** scelto digitandolo nuovamente sul tastierino (vedi immagine 3 sotto).



Ad avvenuta conferma del PIN, sul display appariranno dei trattini lampeggianti indicanti che il token è operativo.

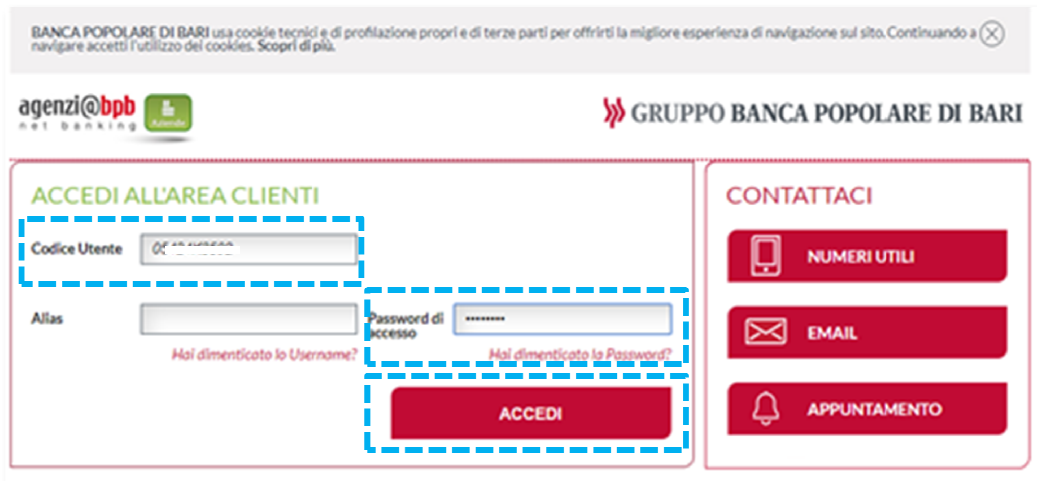


## UTILIZZO DEL TOKEN FISICO con Agenzi@bpb Aziende

Si specifica che quanto di seguito riportato ha valenza sia per l'utenza master che per le utenze secondarie.

### Accedere ad Agenzi@bpb Aziende

1. Collegati ad **agenzi@bpb** Aziende ed esegui l'accesso inserendo "**Username**" e "**Password**" personali quindi clicca su "**Accedi**";



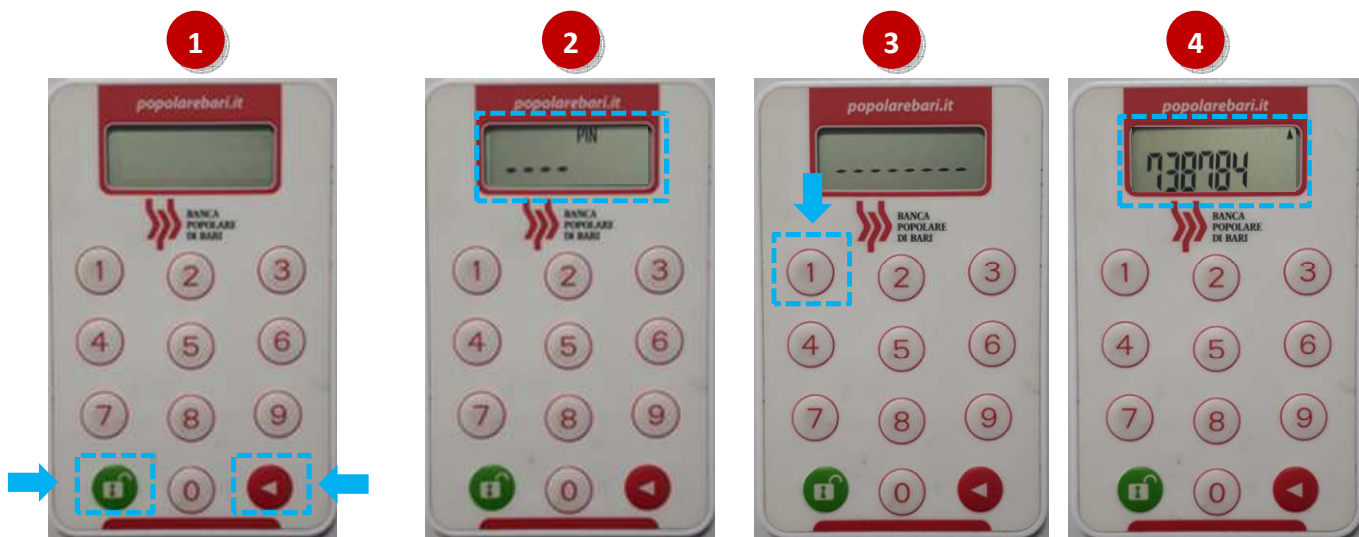
**NOTA BENE:** *Username e Password dell'utente master sono state consegnate al titolare del rapporto in fase di accensione del rapporto telematico. Username e password delle eventuali utenze secondarie sono definite direttamente dall'utente master su agenzi@bpb Aziende. In tale occasione l'utente master associa i seriali dei token fisici ritirati in Filiale alle utenze secondarie generate.*

2. Visualizzerai la pagina di avvio dell'autenticazione tramite Token Fisico ovvero attraverso l'inserimento nel campo "Codice OTP" del codice OTP a 6 cifre generato dalla tua chiavetta fisica.

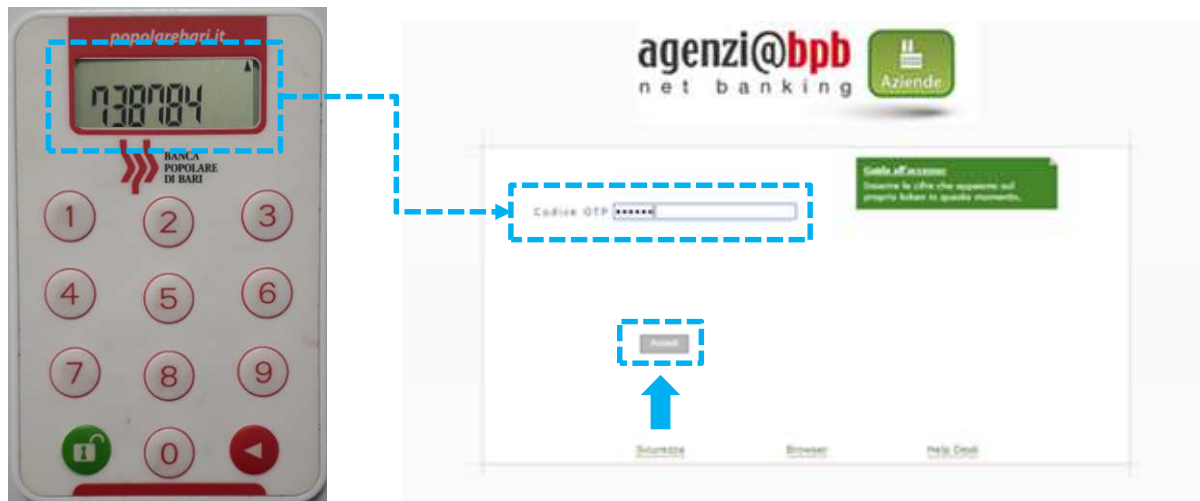


**3.** A questo punto occorre che tu disponga del token fisico per procedere secondo quanto indicato nei prossimi punti e *rappresentato nelle immagini sotto* per generare il codice OTP di accesso:

- 1.** Per attivare il dispositivo, **tieni premuto il tasto rosso e poi premi contemporaneamente il tasto verde** sino a quando non si attiva sul display l'indicazione "**PIN**" (vedi immagine 1 sotto);
- 2.** **Inserisci** il tuo **PIN** personale (vedi immagine 2 sotto);
- 3.** A seguito dell'inserimento del PIN, sul display appariranno dei trattini lampeggianti. **Premere il tasto "1"** per generare il codice OTP di accesso (vedi immagine 3 sotto);
- 4.** **Sul display** verrà visualizzato il codice **OTP a 6 cifre** che utilizzerai per autenticarti ed accedere all'homepage di *agenzi@bpb* (vedi immagine 4 sotto).  
Il codice OTP generato sarà valido 30 sec., tempo entro il quale potrà essere utilizzato. Scaduti i 30 sec. per generare un nuovo OTP dovrai premere nuovamente prima il pulsante rosso quindi il pulsante "1".

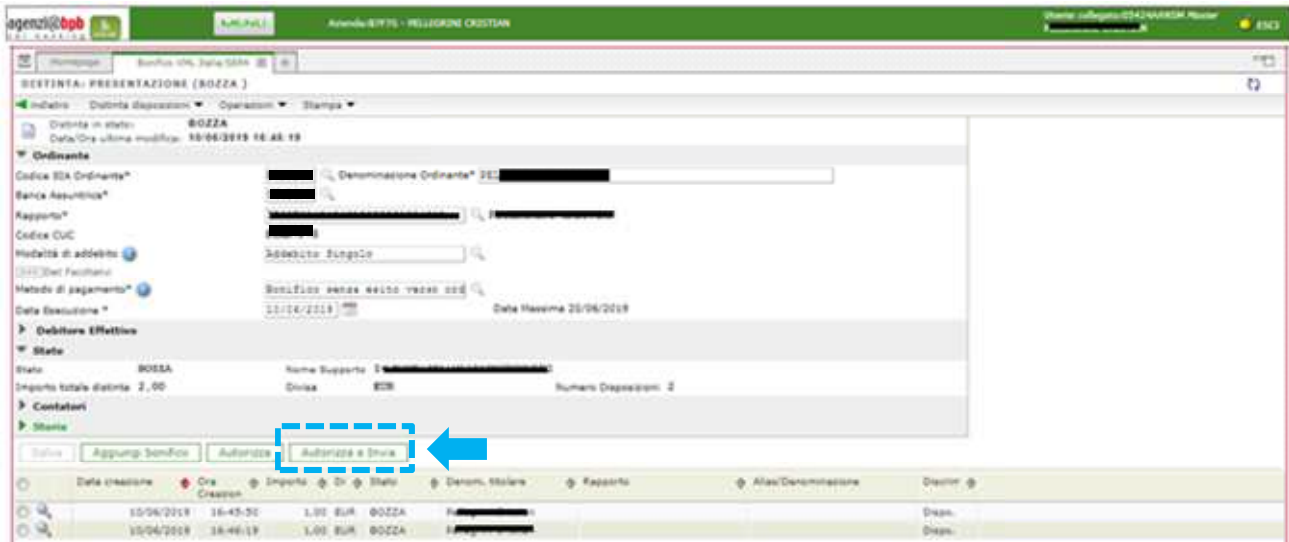


- 5.** **Procedi inserendo** nel campo "**Codice OTP**" della maschera visualizzata sul tuo PC il codice **OTP a 6 cifre** visualizzato sul display del token fisico. **Clicca quindi su "Accedi"** per entrare nella home page di *agenzi@bpb*.

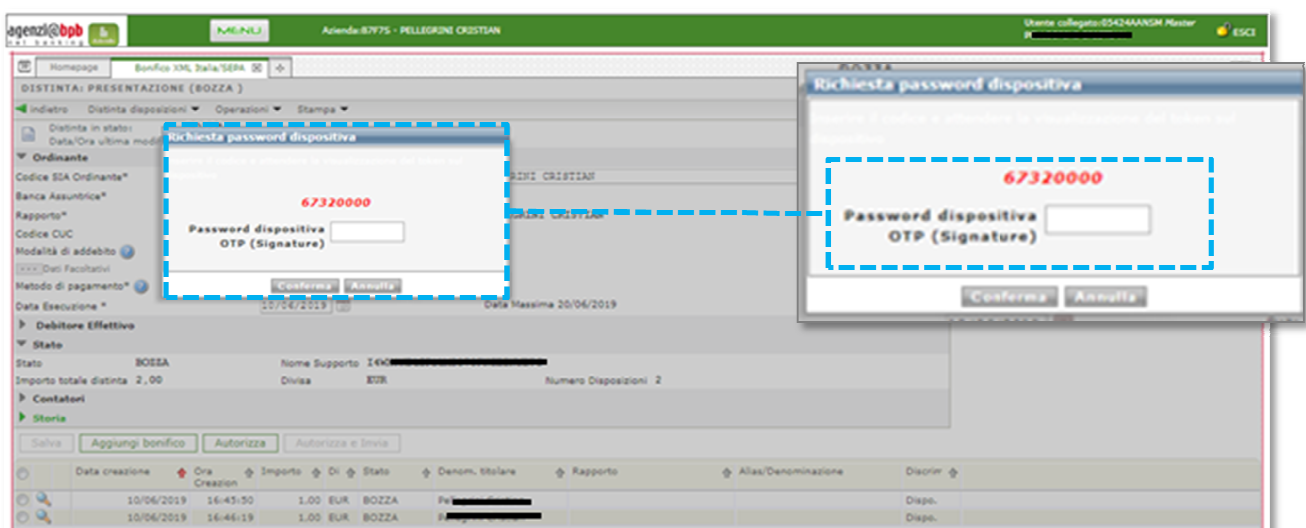


## Autorizzare le disposizioni di pagamento da Agenzi@bpb Aziende

1. Compilata la maschera dell'operazione di pagamento (es. distinta di bonifici, addebiti diretti, etc...), per procedere con l'autorizzazione **clicca** su "**Autorizza e Invia**".



2. A questo punto visualizzerai il Popup "**Richiesta password dispositiva**" che consente di avviare il processo di autorizzazione delle operazioni (in questo esempio una distinta di bonifici) mediante il collegamento dinamico (c.d *Dynamic Linking*). Il popup mostra un **primo codice (in rosso)** collegato univocamente all'operazione come nell'immagine sotto ed il campo "**Password dispositiva OTP (Signature)**" all'interno del quale dovrai inserire il codice prodotto dal Token fisico secondo le indicazioni riportate al punto 3).



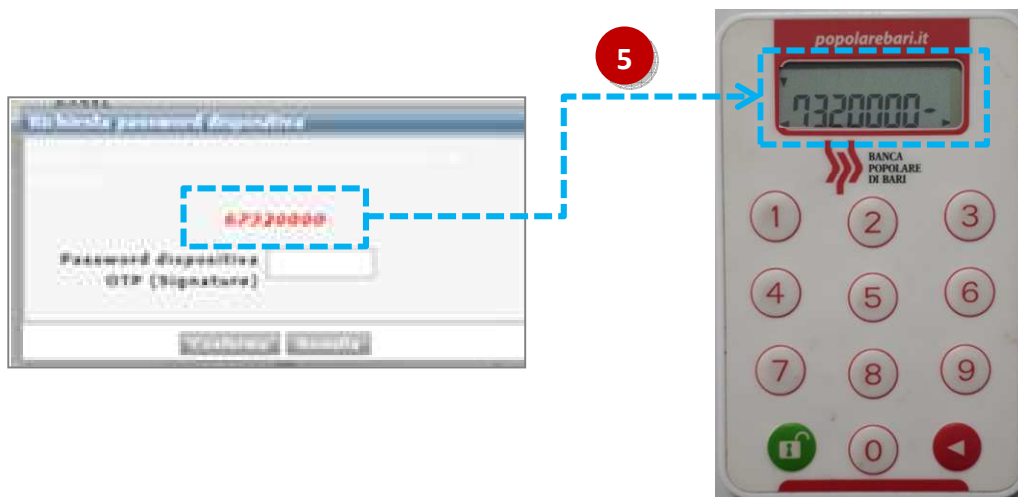


**3.** A questo punto occorre che tu disponga del token fisico per procedere secondo quanto indicato nei prossimi punti, e *rappresentato nelle immagini sotto*, per generare il codice OTP di accesso:

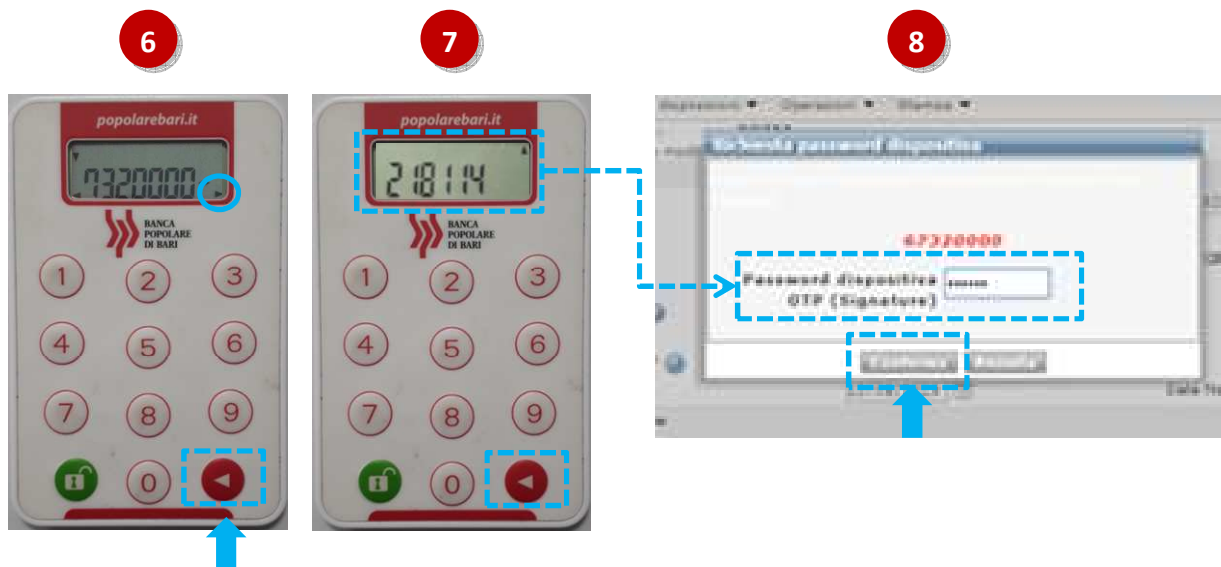
- 1.** Per attivare il dispositivo, **tieni premuto il tasto rosso e poi premi contemporaneamente il tasto verde** sino a quando non si attiva sul display l'indicazione "**PIN**" (vedi immagine 1 sotto);
- 2.** **Inserisci** il tuo **PIN** personale (vedi immagine 2 sotto);
- 3.** A seguito dell'inserimento del PIN, sul display appariranno dei trattini lampeggianti. **Premere il tasto "3"** per avviare la procedura di generazione dell'OTP di firma (vedi immagine 3 sotto);
- 4.** **Il display** del token fisico si predispose per l'inserimento del codice visualizzato, sul PC, nel popup "**Richiesta password dispositiva**" (vedi immagine 4 sotto);



**5.** **Inserisci** sul token fisico il *codice* visualizzato sul monitor del tuo PC come da immagine 5 di seguito riportata;



6. **Tieni premuto il tasto rosso** sino a quando la freccetta visualizzata sul display del token fisico non sarà più visibile (vedi immagine 6 sotto);
7. **Rilascia il tasto rosso** e sul display sarà visualizzato un **codice a 6 cifre** che rappresenta l'**OTP di firma** (c.d dynamic linking) [vedi immagine 7 sotto];
8. **Inserisci** nel **campo "Password dispositiva OTP (Signature)"** del popup visualizzato sul **monitor** del tuo **PC** il **codice a 6 cifre riportato sul display del token fisico** per concludere l'operazione di pagamento e procedere con l'autorizzazione **clickando** su "**Conferma**" (vedi immagine 8 sotto).



A seguito della conferma, le operazioni saranno state autorizzate ed inviate.



## INFORMAZIONI UTILI

### ➤ ASSISTENZA all'UTILIZZO del TOKEN FISICO

Per richieste di assistenza nell'utilizzo del token fisico puoi contattare il **Servizio Clienti** al **Numero Verde 800 005 444** dal lunedì al sabato (lavorativi) dalle 08:00 alle 20:00.

### ➤ RESET del PIN

Nel caso in cui dimenticassi il tuo PIN ovvero nel caso di 5 tentativi consecutivi di errato inserimento potrai richiederne il reset contattando il **Servizio Clienti** al **Numero Verde 800 005 444** dal lunedì al sabato (lavorativi) dalle 08:00 alle 20:00.

Dopo il reset del PIN, al primo utilizzo della chiavetta fisica ti sarà richiesto di impostare un nuovo PIN personale.

### ➤ MODIFICA del PIN

Nel caso in cui tu voglia modificare il PIN in uso, attiva il dispositivo, inserisci il PIN, premi contemporaneamente il tasto rosso ed il tasto verde sino a quando visualizzi sul display l'indicazione "**New Pin**". A questo punto puoi rieseguire la procedura descritta ai punti 2 e 3 del paragrafo PIN e Primo Utilizzo.

### ➤ FURTO o SMARRIMENTO

In caso di smarrimento o furto del token, recati in Filiale per ricevere tutte le istruzioni e ritirare un nuovo dispositivo di autenticazione in modo da garantire la sicurezza della tua operatività.

Per ulteriori informazioni il **Servizio Clienti** al **Numero Verde 800 005 444** dal lunedì al sabato (lavorativi) dalle 08:00 alle 20:00.

### ➤ SBLOCCO ACCOUNT/RESET CREDENZIALI

Per sbloccare il tuo account a seguito di **5 tentativi** di accesso non andati a buon fine, contatta il **Servizio Clienti** al **Numero Verde 800 005 444** dal lunedì al sabato (lavorativi) dalle 08:00 alle 20:00 per ripristinare la password di primo accesso ricevuta in fase di sottoscrizione del contratto di Corporate Banking Interbancario.