



SOCIETA' PER AZIONI - SEDE IN CASTELLAMMARE DI STABIA

## INTERNET BANKING

### GUIDA AI SERVIZI

Gentile Cliente,

questo documento contiene importanti informazioni sul servizio Internet Banking che lei utilizza attraverso le applicazioni Internet Banking Desktop (da PC) e/o Mobile Banking (smartphone e tablet) messe a disposizione dalla Banca. La invitiamo a leggere con attenzione.

Il Regolamento europeo 2018/389 (decorrenza 14.09.2019) impone nuovi requisiti per l'autenticazione del cliente che opera a distanza con la finalità di accrescere la sicurezza dei pagamenti e ridurre il fenomeno delle frodi.

L'autenticazione è la procedura con cui la Banca accerta l'identità del cliente che accede al servizio di Internet Banking e autorizza le operazioni.

La Banca adotta da tempo - e mantiene costantemente aggiornati - elevati standard di sicurezza per i servizi di Internet Banking, ricorrendo a sistemi di autenticazione sicura del cliente al fine di ridurre il rischio di frode.

In questo contesto, il Regolamento europeo impone l'adozione di sistemi di autenticazione del cliente ancora più avanzati, che prevedono l'autorizzazione di ciascuna operazione tramite l'utilizzo di un codice dinamico univocamente legato al beneficiario e all'importo della singola operazione.

All'atto di sottoscrizione del contratto è indispensabile che il Cliente indichi il suo numero di cellulare e la sua e-mail.

**Per accedere al servizio Internet Banking è prioritariamente necessario disporre di un CODICE UTENTE e di una PASSWORD.**

- CODICE UTENTE: Le viene inoltrato all'atto di sottoscrizione del contratto a mezzo mail;
- PASSWORD: Le viene fornita una PASSWORD INIZIALE in cartaceo all'atto di sottoscrizione del contratto che necessariamente deve essere modificata al primo accesso e conservata con la massima cura.

Inoltre, l'attuale sistema tecnologico di autenticazione per il Servizio di Internet Banking prevede i più avanzati sistemi (**alternativi tra loro**):

- "Token Sw RSA TS100S" denominato **TOKEN VIRTUALE**
- "Token Hw Vasco DP270" denominato **TOKEN FISICO**

In fase di stipula del contratto il cliente ne indica la scelta.

I due schemi di autenticazione possibili prevedono differenti modalità di generazione dei codici di sicurezza, sia al Login (dopo la digitazione di "nome utente" e "password") sia in fase autorizzativa:

- Il TOKEN VIRTUALE (Token Sw RSA TS100S) prevede OTP con pin al login e firma di transazioni con payload (contenuto della richiesta) in fase autorizzativa;
- Il TOKEN FISICO (Token Hw Vasco DP270) prevede OTP semplice al login, e OTP di firma in fase autorizzativa.

## Token Sw RSA TS100S – TOKEN VIRTUALE

Il Token Sw RSA TS100S è utilizzabile con uno smartphone o con un tablet dotato di connessione dati.

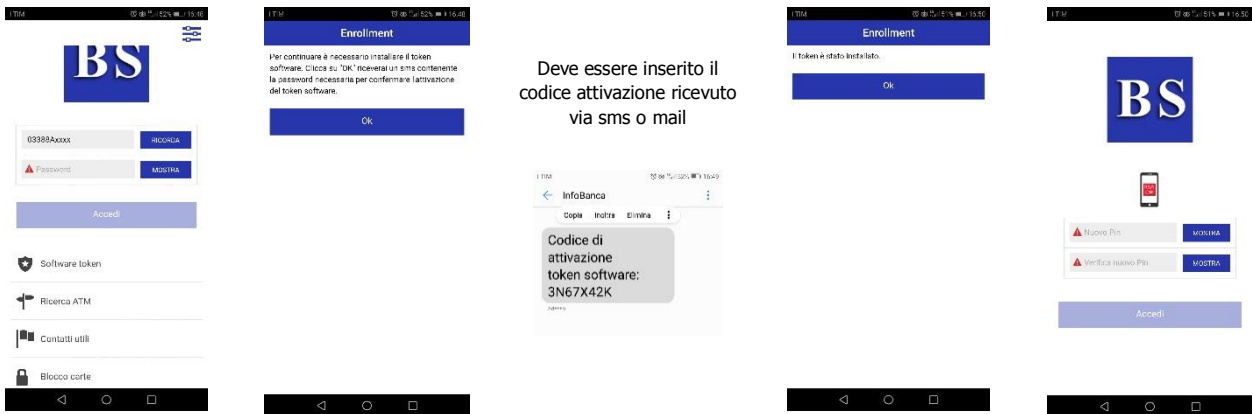
I codici dinamici per accedere al servizio Internet Banking e per autorizzare operazioni verranno generati tramite l'app Banca Stabiese a seguito della digitazione del PIN.

### PRIMO ACCESSO (Attivazione) Enrollment Software Token TS100S (solo da App Mobile)

Eseguendo il primo accesso dall'APP (dopo aver inserito le credenziali) il sistema invierà all'utente una CODICE DI ATTIVAZIONE tramite SMS (e/o Mail), che dovrà essere inserita nell'apposito campo dell'applicazione per completare l'attivazione (enrollment).

Al termine dell'enrollment del token, se necessario, sarà proposta l'inizializzazione del pin del token. Dovrà essere creato a scelta dell'utente un PIN numerico di 4 numeri.

Nelle schermate seguenti viene dettagliato il flusso previsto per completare l'enrollment.



### Utilizzo tramite App Mobile con token installato

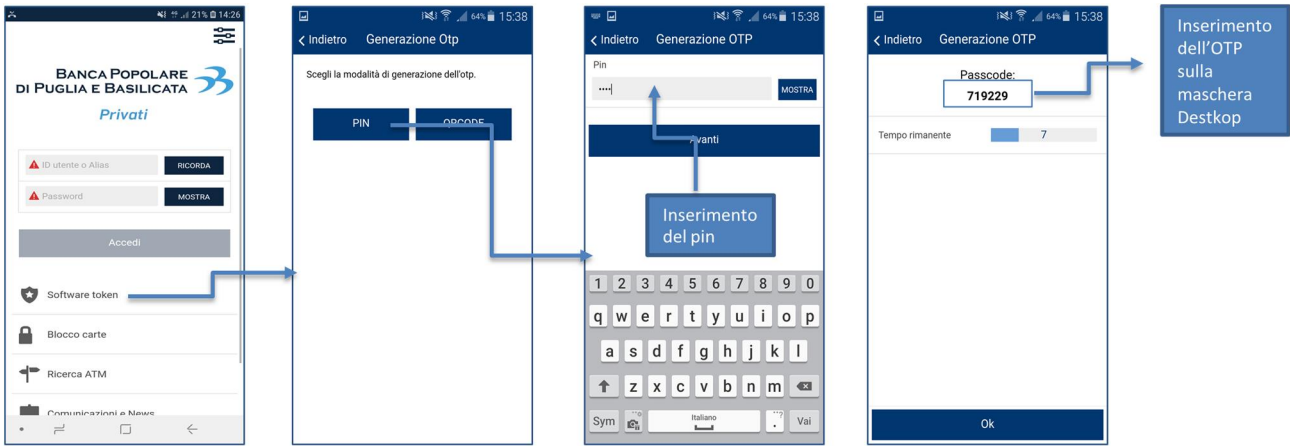
All'utente viene richiesto l'inserimento del PIN per l'autorizzazione delle operazioni. La generazione della signature è trasparente all'utente.

### Utilizzo tramite Internet Banking Desktop PC, con token installato su App Mobile

- **accesso**

Dopo aver inserito le Credenziali nella apposita area riservata del sito della Banca, il cliente dovrà aprire l'app, selezionare la funzione "Software Token", selezionare la modalità «OTP» nelle opzioni presentate, introdurre il PIN; il sistema genera un **passcode** da inserire sull'IHB desktop (PC).





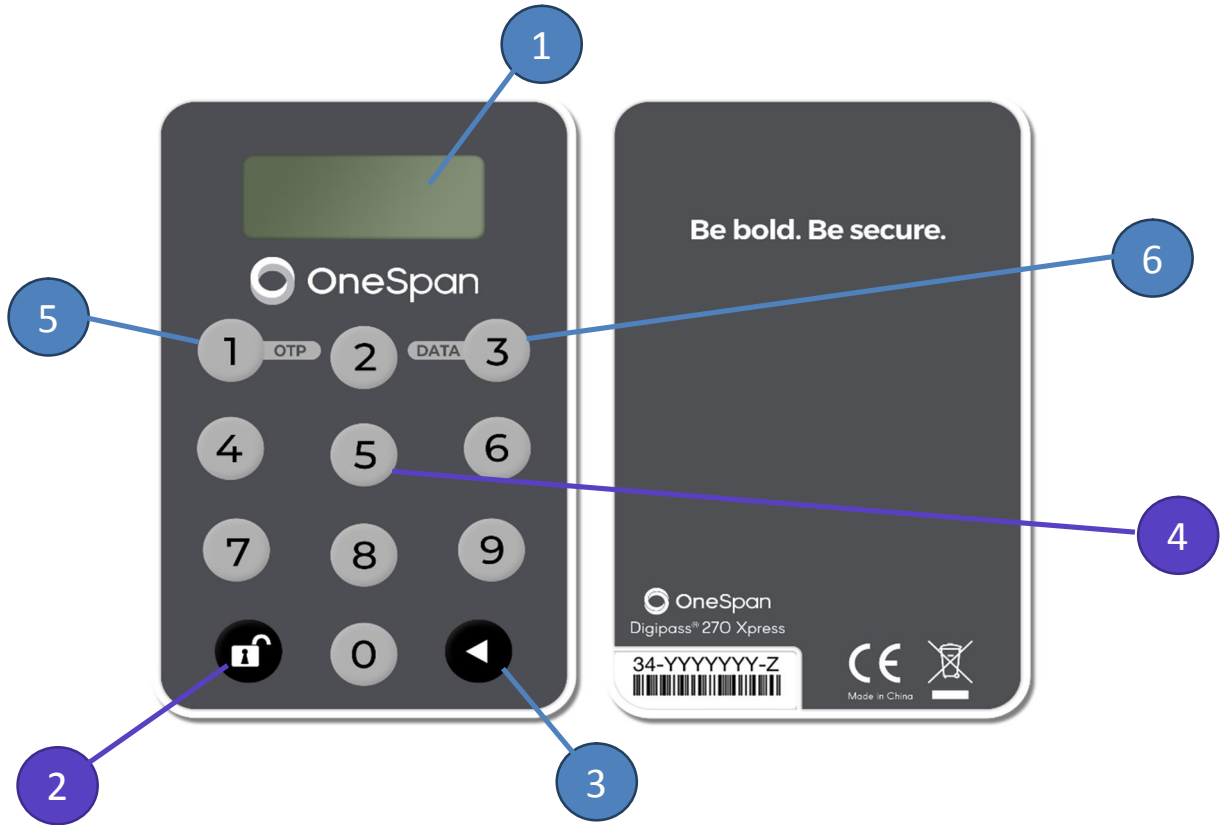
**- Inserimento disposizioni**

Per quanto concerne l'autorizzazione delle disposizioni, la sezione di sicurezza della videata dell'Internet Banking desktop (PC) mostrerà un codice QR-code. L'utente dovrà utilizzare l'app home banking sul proprio smartphone/tablet, selezionare la funzione "Software Token" e selezionare la modalità di utilizzo «QR Code» e inquadrare il codice QR-code presente sull'Internet Banking Desktop (PC). Sullo smartphone verrà mostrata una descrizione dell'operazione che si sta autorizzando e verrà richiesta la digitazione del PIN personale per generare il codice dispositivo dell'operazione. L'utente dovrà inserire tale codice nella schermata dell'Internet banking Desktop (PC) nel campo dedicato alla digitazione del Token, e confermare l'autorizzazione della disposizione.



**Token Hw Vasco DP270 - TOKEN FISICO**


Il dispositivo dispone di un display grafico, per consentire l’inserimento e la visualizzazione dei dettagli della transazione (ad esempio beneficiario ed ammontare come richiesto dalla PSD 2 per il dynamic linking) in modo chiaro e trasparente e guidare facilmente l’utente nell’utilizzo.



1	Schermo
2	Bottone di sbocco per accensione
3	Bottone di Accensione/Spegnimento
4	Keypad inserimento dati
5	Tasto 1 applicazione OTP Semplice
6	Tasto 3 applicazione Dynamic Linking

Il dispositivo Vasco DP270 si accende tramite la seguente combinazione di tasti

Tenendo premuto il tasto  premere il tasto 

Per spegnere il dispositivo premere il tasto 

Il dispositivo si spegne automaticamente dopo 30 secondi di inattività.

- **Accesso**

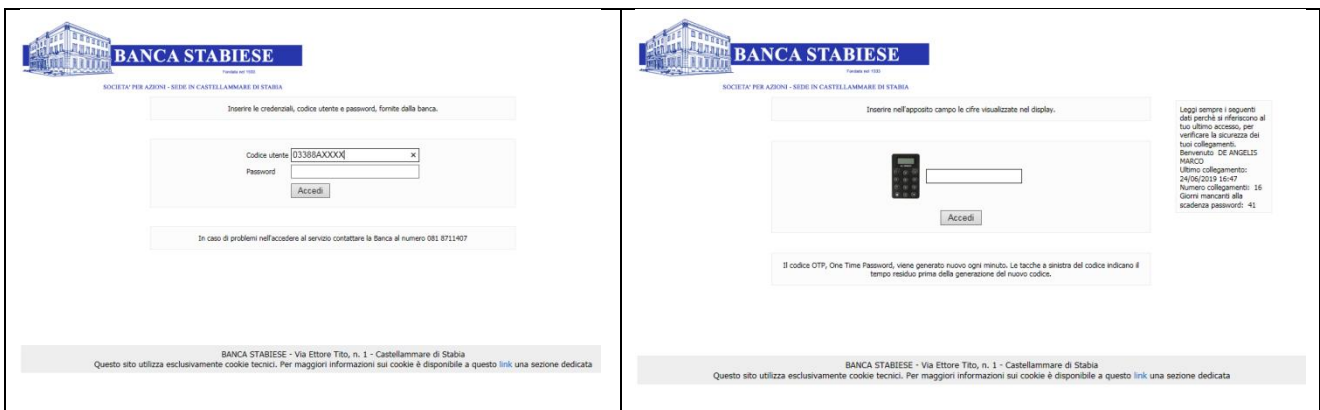
L'utente deve prima inserire le credenziali iniziali (codice utente e password). Poi verrà proposta la schermata in cui inserire il codice OTP generato dispositivo Vasco DP270.

Dopo aver acceso il dispositivo, premere il tasto **1**

Il dispositivo mostra la OTP generata:



Premendo il tasto  per tornare al menu principale.




- **Disposizioni**

Con dispositivo acceso, premere il tasto **3**

L'utente tramite il tastierino numerico del diapositivo digita il codice proposto in fase di autorizzazione della disposizione (dati relativi a beneficiario e ammontare)



Nel caso in cui occorra modificare il valore inserito premere il tasto  per cancellare i dati.

Successivamente è possibile generare la OTP tenendo premuto per più di 1 secondo il tasto 



Infine, per completare l'operazione, inserire tale codice numerico nell'apposito campo relativo a tale disposizione.