

## **ISTRUZIONI OPERATIVE dei sistemi di generazione di codici dinamici resi disponibili dalla Banca**

- 1. "Secure Call"**
- 2. "BG Token"**

### **1. Istruzioni operative per l'utilizzo della funzionalità "Secure Call"**

La funzionalità "Secure Call", che protegge da possibili attacchi di phishing conseguenti ad intrusioni nel sistema (cd. man in the middle e man in the browser) e che utilizza il telefono cellulare del Cliente come token di riconoscimento, è regolata dalle seguenti istruzioni operative, che il Cliente dichiara di aver letto, compreso ed accettato:

1. Attraverso l'attivazione della funzionalità "Secure Call", messa a disposizione dalla Banca nell'ambito del Servizio di Internet Banking, il Cliente potrà - nelle modalità esposte ai punti successivi - accedere alla propria area riservata del sito [www.bancagenerali.it](http://www.bancagenerali.it) e confermare le operazioni che intende effettuare, in conformità a quanto dalle parti pattuito in sede di stipula del contratto. Per alcune specifiche tipologie di operazioni, puntualmente individuate nella Sezione "Gestione Profilo" all'interno dell'Area Riservata del sito [www.bancagenerali.it](http://www.bancagenerali.it), il Cliente potrà altresì optare per una modalità di conferma alternativa<sup>1</sup>.

2. In fase di accesso all'area riservata, apparirà sullo schermo del dispositivo utilizzato dal Cliente per la navigazione un avviso contenente un numero verde, un codice a quattro cifre ("One Time Password" - "OTP") e l'indicatore di stato della richiesta; il Cliente dovrà comporre dal proprio cellulare il numero verde indicato e, in base alle istruzioni dell'albero vocale, digitare la OTP; il processo di autorizzazione andrà a buon fine se la chiamata sarà stata effettuata con il cellulare abilitato dal Cliente per l'operatività e se la OTP risulterà digitata correttamente.

3. In fase di conferma delle operazioni, il processo di autorizzazione sarà lo stesso indicato al precedente punto 2, ad eccezione delle operazioni di pagamento in ambito PSD2<sup>2</sup> relativamente a conti correnti e carte di pagamento (es. bonifico o ricarica carta prepagata), per le quali sarà richiesto di digitare una OTP aggiuntiva (sempre di 4 cifre e visualizzata sullo schermo del dispositivo del Cliente), che verrà generata sulla base dell'operazione che si sta effettuando. Dopo aver seguito i passaggi riportati nel punto 2, la voce registrata continuerà riepilogando i dati dell'operazione e, se questi sono corretti, sarà possibile darne conferma digitando l'OTP mostrata sul dispositivo del Cliente e attendere la chiusura automatica della chiamata.

4. Il Cliente che opera dall'estero dovrà indicare tale circostanza nell'apposito campo in sede di conferma dell'operazione; in tal caso - a differenza di quanto descritto ai punti 3 e 4 - il Cliente riceverà una telefonata sul cellulare abilitato e, seguendo le istruzioni, dovrà digitare correttamente l'OTP richiesta (es. data di nascita) oppure l'OTP mostrata sullo schermo del dispositivo del Cliente.

Si ricorda che i costi della telefonata dal confine italiano al paese estero in cui si trova il Cliente saranno ad esclusivo carico di quest'ultimo, in linea con la prassi telefonica internazionale.

5. L'operatività fin qui descritta può essere posta in essere anche sull'APP di Banca Generali e sul mobile site [my.bancagenerali.it](http://my.bancagenerali.it), grazie al Servizio Mobile Banking, che supporta tale funzionalità di sicurezza.

6. Qualora il Cliente avesse subito il furto della SIM ovvero l'avesse smarrita, dovrà contattare il Numero Verde 800.133.133, operativo dalle ore 8.00 alle ore 22.00 dal lunedì al venerdì ed il sabato dalle ore 8.00 alle ore 14.00.

7. Il Cliente potrà variare il numero di utenza telefonica abilitato alla funzionalità "Secure Call" utilizzando l'apposito modulo messo a disposizione dalla Banca oppure attraverso altre modalità tempo per tempo messe a disposizione dalla Banca stessa.

8. La cessazione, per qualsiasi causa, dell'accesso al Servizio di Internet Banking comporta l'automatica cessazione della funzionalità "Secure Call".

---

<sup>1</sup> Password dispositiva dal Cliente stesso creata (Secure Code).

<sup>2</sup> Direttiva 2015/2366/UE del 25 novembre 2015, recepita in Italia con il D.Lgs. 15 dicembre 2017, n.218.

## 2. Istruzioni operative per l'utilizzo della funzionalità "BG Token"

La funzionalità "BG Token" utilizza un dispositivo del Cliente come token di riconoscimento ed è regolata dalle seguenti istruzioni operative, che il Cliente dichiara di aver letto, compreso ed accettato:

1. Attraverso l'attivazione della funzionalità "BG Token", messa a disposizione dalla Banca nell'ambito del Servizio di Internet Banking, il Cliente potrà - nelle modalità esposte ai punti successivi - accedere alla propria area riservata del sito [www.bancagenerali.it](http://www.bancagenerali.it) e confermare le operazioni che intende effettuare, in conformità a quanto dalle parti pattuito in sede di stipula del contratto. Per alcune specifiche tipologie di operazioni, puntualmente individuate nella Sezione "Gestione Profilo" all'interno dell'Area Riservata del sito [www.bancagenerali.it](http://www.bancagenerali.it), il Cliente potrà altresì optare per una modalità di conferma alternativa<sup>2</sup>.

2. L'app "BG Token" deve essere scaricata dal Cliente sul proprio dispositivo (fino a un massimo di 5 diversi dispositivi) accedendo allo store di riferimento (App Store per iOS o Play Store per Android). Dopo l'installazione, l'app dovrà essere associata al Cliente: per procedere, si dovrà utilizzare [questo collegamento](https://www.bancagenerali.it/ebenroll/ib/login?abi=03075&brand=0) (<https://www.bancagenerali.it/ebenroll/ib/login?abi=03075&brand=0>), che sarà presente al termine della personalizzazione del profilo di sicurezza, nella pagina di login per l'Area Riservata del sito [www.bancagenerali.it](http://www.bancagenerali.it) e sul sito [www.bancageneraliprivate.it](http://www.bancageneraliprivate.it). Per accedere sarà obbligatorio inserire le stesse credenziali di autenticazione utilizzate per l'Area Riservata [www.bancagenerali.it](http://www.bancagenerali.it).

3. All'interno della piattaforma di registrazione di "BG Token", il Cliente dovrà selezionare il numero di telefono cellulare (tra quelli comunicati alla Banca e quindi presenti in anagrafica) sul quale ricevere il codice a quattro cifre ("One Time Password" – "OTP") per validare l'attivazione. Il Cliente inserirà sul dispositivo, nella sezione "Attiva BG Token", il Numero Identificativo e il Codice Autorizzativo (mostrati sullo schermo del dispositivo del Cliente) e la Password di Attivazione (ricevuta via SMS sul telefono cellulare di cui al precedente punto 2). Dopo questa procedura, l'app "BG Token" sarà correttamente associata al Cliente.

4. Dopo l'attivazione, il Cliente dovrà impostare una password per l'app "BG Token" (minimo 4 e massimo 6 caratteri), che non dovrà essere debole (es. 123456). L'app richiederà inoltre di impostare la biometria come modalità di autenticazione (impronta digitale o FaceID) sui dispositivi supportati.

5. In fase di accesso all'area riservata e conferma delle operazioni, comparirà sullo schermo del Cliente la scelta tra due modalità di autenticazione:

- Online: il dispositivo mobile registrato dal cliente dispone di una connessione Internet e può quindi ricevere notifiche "push" (previa autorizzazione tramite le impostazioni del dispositivo stesso). Il Cliente riceverà la notifica sul dispositivo registrato e potrà inserire la biometria (o la password) per visualizzare l'operazione da confermare; potrà quindi selezionare "Conferma" o "Rifiuta" per procedere con l'operatività confermando tramite biometria (o la password).
- Offline: il dispositivo mobile registrato non dispone di una connessione Internet e il Cliente dovrà entrare sull'app "BG Token" e selezionare "Inquadra il codice" per generare un codice temporaneo (OTP) per confermare l'accesso o le operazioni, che verrà inserito nell'apposito campo nell'Area Riservata su [www.bancagenerali.it](http://www.bancagenerali.it). Questa opzione non è presente sull'APP di Banca Generali, in quanto per poter navigare è un prerequisito necessario disporre di una connessione Internet.

6. Il Cliente che opera dall'estero seguirà le indicazioni del punto 4. Si ricorda che i costi di connessione dal confine italiano al paese estero in cui si trova il Cliente saranno ad esclusivo carico di quest'ultimo, in linea con la prassi telefonica internazionale.

7. L'operatività fin qui descritta può essere posta in essere anche sull'APP di Banca Generali e sul mobile site [my.bancagenerali.it](http://my.bancagenerali.it), grazie al Servizio Mobile Banking, che supporta tale funzionalità di sicurezza.

8. Esclusivamente per il Cliente che ha scelto BG Token e il cui conto è stato aperto in modalità digitale<sup>3</sup> sarà possibile utilizzare l'app BG Token per autorizzare le disposizioni tramite Phone Banking: dopo aver dato le indicazioni dell'operazione che si vuole effettuare all'operatore del Customer Care, per autorizzarla sarà richiesto di comunicare un codice temporaneo (OTP) che verrà generato utilizzando la funzionalità nell'app

---

<sup>2</sup> Password dispositiva dal Cliente stesso creata (Secure Code).

<sup>3</sup> Si intende il Cliente che ha utilizzato la piattaforma di apertura conto digitale in autonomia oppure a cui è stato aperto il conto digitalmente, scegliendo quindi l'invio digitale dei codici per l'accesso.

BG Token «*Genera password temporanea per operare con il Customer Care*». Il codice da comunicare ha validità di 60 secondi: una volta scaduto il tempo, è necessario richiedere la generazione di un nuovo codice per poter terminare l'operazione. Per quanto qui non previsto, si rinvia alla Normativa Contrattuale sottoscritta dal Cliente relativa al servizio Phone Banking ("Seconda Sezione" del contratto - Documento C. "Norme che regolano il servizio Phone Banking").

9. Qualora il Cliente avesse subito il furto del telefono cellulare su cui ha installato l'app "BG Token" ovvero l'avesse smarrito dovrà contattare il Numero Verde 800.133.133, operativo dalle ore 8.00 alle ore 22.00 dal lunedì al venerdì e il sabato dalle ore 8.00 alle ore 14.00.

10. La cessazione, per qualsiasi causa, dell'accesso al Servizio di Internet Banking comporta l'automatica cessazione della funzionalità "BG Token".