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

Con l'emanazione delle norme tecniche di regolamentazione della Direttiva Europea PSD2[1] in tema di autenticazione del Cliente e conferma delle operazioni bancarie, per assicurare un alto standard di sicurezza, sarà richiesto al Cliente di effettuare un'autenticazione forte sia per accedere a tutte le piattaforme digitali della Banca sia per confermare le operazioni. Le due modalità di autenticazione forte sono le seguenti:

1. **"Mobile Token"** (impostazione di default del profilo al primo accesso)
2. **"Secure Call"**

1. Istruzioni operative per l'utilizzo della funzionalità "Mobile Token"

La funzionalità "Mobile Token", che migliora la protezione da possibili attacchi di phishing conseguenti ad intrusioni nel sistema (come, a titolo esemplificativo e non esaustivo, man in the middle e man in the browser) e che utilizza un dispositivo del Cliente come token di riconoscimento, è regolata dalle seguenti istruzioni operative, che il Cliente dichiara di aver letto, compreso e accettato:

1. Attraverso l'attivazione della funzionalità "Mobile 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 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 di investimento (non rientranti nel perimetro della Direttiva Europea PSD2), puntualmente individuate nell'Area Riservata del sito www.bancagenerali.it e nel sito www.bancageneraliprivate.it, il Cliente potrà altresì optare per una modalità di conferma alternativa[2]. Inoltre, esclusivamente per le operazioni di compravendita titoli dall'Area Riservata del sito www.bancagenerali.it, la conferma avverrà in modalità "one-click", senza necessità di effettuare la conferma tramite la funzionalità "Mobile Token" o password dispositiva (tale modalità non è al momento disponibile sull'APP "Banca Generali Private").

2. Per l'attivazione della funzionalità "Mobile Token", il Cliente deve scaricare l'APP "Banca Generali Private" (di seguito "APP") sul proprio dispositivo accedendo allo store di riferimento (App Store per iOS o Play Store per Android). Dopo l'installazione, l'APP dovrà essere associata al Cliente. L'APP può essere attivata con Mobile Token su 5 dispositivi diversi: raggiunto il numero massimo sarà necessario effettuare il reset di tutti i dispositivi (guidato dall'APP) per poter riprendere con una nuova attivazione.

3. Per attivare la funzionalità "Mobile Token" sul profilo del Cliente, sarà necessario effettuare l'accesso sull'APP tramite le credenziali di autenticazione utilizzate per l'Area Riservata del sito www.bancagenerali.it e selezionare il numero di telefono cellulare (tra quelli comunicati alla Banca, quindi presenti in anagrafica e sul quale è stata attivata almeno una volta la funzionalità "Secure Call") su cui ricevere il codice a quattro cifre ("One Time Password" – "OTP") per validare l'attivazione.

4. Il Cliente dovrà impostare una "Token Password" (di 6 caratteri). La "Token Password" è necessaria per utilizzare la funzionalità "Mobile Token" e confermare le operazioni tramite "Mobile Token". La Token Password potrà contenere lettere, numeri e/o caratteri speciali e dovrà presentare dei livelli minimi di complessità (per esempio, non potrà contenere caratteri/numeri la cui differenza è costante, come "123456" o "111111").

5. Dopo aver completato l'attivazione, in fase di accesso all'APP, sarà chiesto al Cliente se vuole attivare il riconoscimento biometrico, oltre che per l'accesso in APP, anche per la conferma delle operazioni tramite "Mobile Token". L'attivazione o la disattivazione del riconoscimento biometrico è possibile in ogni momento accedendo alle Impostazioni dell'APP.

6. In fase di accesso all'Area Riservata del sito e conferma delle operazioni in modalità web, comparirà sullo schermo del Cliente la scelta tra due modalità di autenticazione:

- Online: il dispositivo mobile attivato dal Cliente dispone di una connessione Internet e può quindi ricevere notifiche "push" (autorizzazione modificabile tramite le impostazioni del dispositivo stesso). Il Cliente riceverà la notifica sul dispositivo e potrà inserire la biometria (o la "Token Password") per

[1] Direttiva 2015/2366/UE del 25 novembre 2015, recepita in Italia con il D.Lgs. 15 dicembre 2017, n.218

[2] Password dispositiva dal Cliente stesso creata (Secure Code)

visualizzare l'operazione da confermare; potrà quindi autorizzare o rifiutare l'operatività confermando tramite biometria (o la "Token Password").

- Offline: il dispositivo mobile attivato non dispone di una connessione Internet e il Cliente dovrà entrare sull'APP, accedere alla funzionalità veloce "Mobile Token" e selezionare l'apposita funzionalità che permette l'operatività offline per generare un codice temporaneo (OTP) tramite l'utilizzo della propria fotocamera per confermare l'accesso o le operazioni, che dovrà essere inserito nell'apposito campo nell'Area Riservata su www.bancagenerali.it. Questa opzione non è presente sull'APP, in quanto per poter navigare è un prerequisito necessario disporre di una connessione Internet.

7. Il Cliente che opera dall'estero seguirà le indicazioni del punto 6. 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.

8. L'operatività fin qui descritta può essere posta in essere anche sul mobile site del sito www.bancagenerali.it, grazie al Servizio Mobile Banking, che supporta tale funzionalità di sicurezza.

9. La conferma degli accessi e delle operazioni sull'APP "Banca Generali Private" sarà possibile utilizzando la biometria (o la "Token Password").

10. Esclusivamente per il Cliente che ha scelto "Mobile Token" e il cui conto è stato aperto in modalità digitale[3] oppure ha chiesto la riemissione dei codici in modalità digitale sarà possibile utilizzare l'APP "Banca Generali Private" 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 l'apposita funzionalità all'interno del "Mobile Token" che permette l'operatività tramite Customer Care. Il codice da comunicare ha validità di 60 secondi. 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").

11. Qualora il Cliente avesse subito il furto del telefono cellulare su cui ha installato l'APP "Banca Generali Private" ovvero l'avesse smarrito dovrà contattare il Numero Verde 800.133.133, operativo dalle ore 8.00 alle ore 20.00 dal lunedì al venerdì e il sabato dalle ore 8.00 alle ore 14.00.

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

2. Istruzioni operative per l'utilizzo della funzionalità "Secure Call"

La funzionalità "Secure Call", che migliora la protezione da possibili attacchi di phishing conseguenti ad intrusioni nel sistema (come, a titolo esemplificativo e non esaustivo, 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 e 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 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 di investimento (non rientranti nel perimetro della Direttiva Europea PSD2), puntualmente individuate nell'Area Riservata del sito www.bancagenerali.it e nel sito www.bancageneraliprivate.it, il Cliente potrà altresì optare per una modalità di conferma alternativa[4]. Inoltre, esclusivamente per le operazioni di compravendita titoli dall'Area Riservata del sito www.bancagenerali.it, la conferma avverrà in modalità "one-click", senza necessità di effettuare la conferma tramite la funzionalità "Secure Call" o password dispositiva (tale modalità non è al momento disponibile sull'APP "Banca Generali Private").

[3] 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 l'invio digitale dei codici per l'accesso.

[4] Password dispositiva dal Cliente stesso creata (Secure Code)

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, a eccezione delle operazioni di pagamento in ambito PSD2 relativamente a conti correnti e carte di pagamento (per esempio, 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 "Banca Generali Private" e sul mobile site del sito www.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 20.00 dal lunedì al venerdì ed il sabato dalle ore 8.00 alle ore 14.00, oltre a contattare il proprio gestore telefonico per segnalare l'evento.

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".