GUIDA ALL'UTILIZZO DEI SERVIZI BANCARI ONLINE

aggiornata al 29 luglio 2019

In questa guida ti forniamo indicazioni operative sull'utilizzo degli strumenti di sicurezza del tuo conto, seguite da informazioni utili alla sicurezza online e alla protezione della tua identità digitale.

INDICE

1. AUTENTICARSI IN SICUREZZA PER UTILIZZARE L'HOME BANKING

Le modalità di autenticazione all'home banking della CSR variano a seconda del dispositivo di sicurezza associato al tuo contratto telematico.
La Cassa ti dà la possibilità di scegliere lo strumento più adatto alle tue esigenze, tra Token virtuale e Secure call.
Il presupposto in entrambi i casi è che tu sia in possesso di un telefono cellulare e di un numero telefonico con prefisso italiano.

Il **Token virtuale** è uno strumento di autenticazione integrato nell'APP mobile della CSR. Per utilizzarlo, quindi, devi disporre di uno smartphone e devi scaricare l'APP della CSR, disponibile gratuitamente, per iOS e Android, su App Store e Google Play.
Il Token virtuale può essere utilizzato sia se operi da desktop sia se operi dall'APP mobile stessa. Se hai accettato la soluzione Token virtuale - assegnata di default dalla Cassa - leggi i Capitoli 2 e 4 di questa guida.

La **Secure call** è uno strumento di autenticazione utilizzabile con un qualunque telefono cellulare. A differenza del Token virtuale, non devi disporre di uno smartphone; come il Token virtuale, anche la Secure call può essere utilizzata sia se operi da desktop che dall'app mobile.
Se vuoi scegliere la soluzione Secure call, vai al Capitolo 3.1.
Se hai già scelto la Secure call e vuoi imparare ad usarla, leggi i Capitoli 3.2, 3.3 e 5.

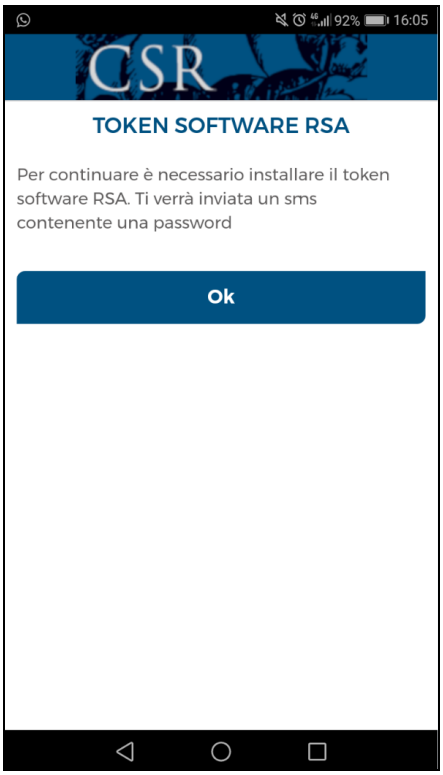
2. ACCEDERE CON IL TOKEN VIRTUALE

2.1 ATTIVARE IL TOKEN VIRTUALE

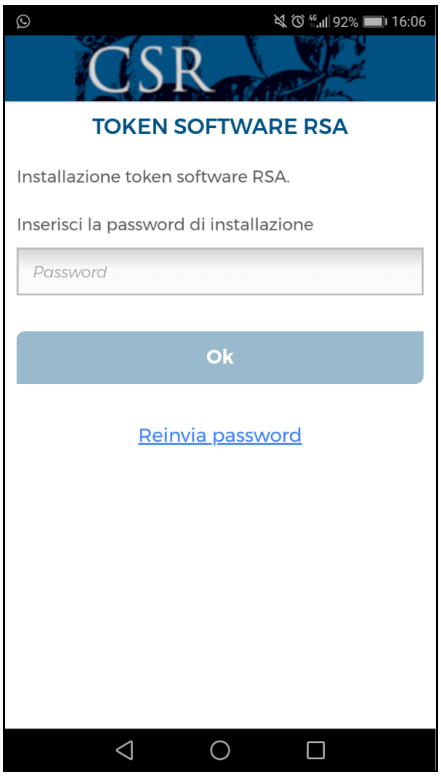
Se alla tua utenza di home banking è stato attribuito lo schema "Token virtuale", dovrai "certificare" l'APP affinché sia univocamente associata all'utenza stessa.
Prima di iniziare, verifica che data e ora siano correttamente impostate sul tuo smartphone e attivane l'impostazione automatica. Inoltre, se ti viene richiesto di abilitare l'APP della CSR all'uso della fotocamera, premi su CONSENTI:

Entra nell'APP, inserisci la Username e la Password dell'home banking e premi su ACCEDI:

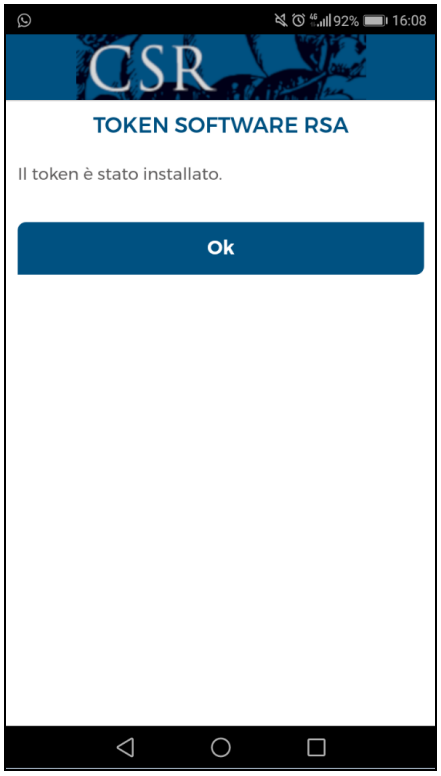
La prima volta che accedi all'APP ti verrà chiesto di installare il Token virtuale. Premi su OK:



Inserisci la password che hai ricevuto tramite SMS, facendo attenzione a maiuscole e minuscole, e premi su OK:

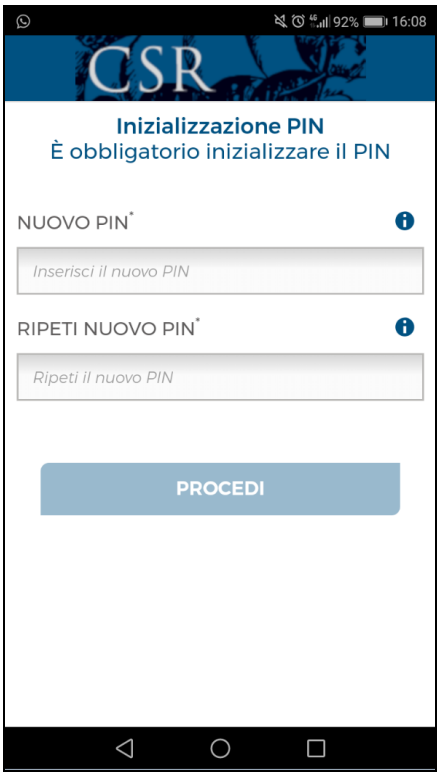


Se non ricevi l'SMS leggi le FAQ per verificare a cosa può essere dovuto il problema.
Se, invece, l'installazione è andata a buon fine, apparirà il seguente messaggio di conferma.
Premi su OK:



Installato il Token virtuale, devi scegliere un codice PIN che ti servirà per utilizzarlo.
Entra nell'APP, inserisci la Username e la Password dell'home banking e premi su ACCEDI:

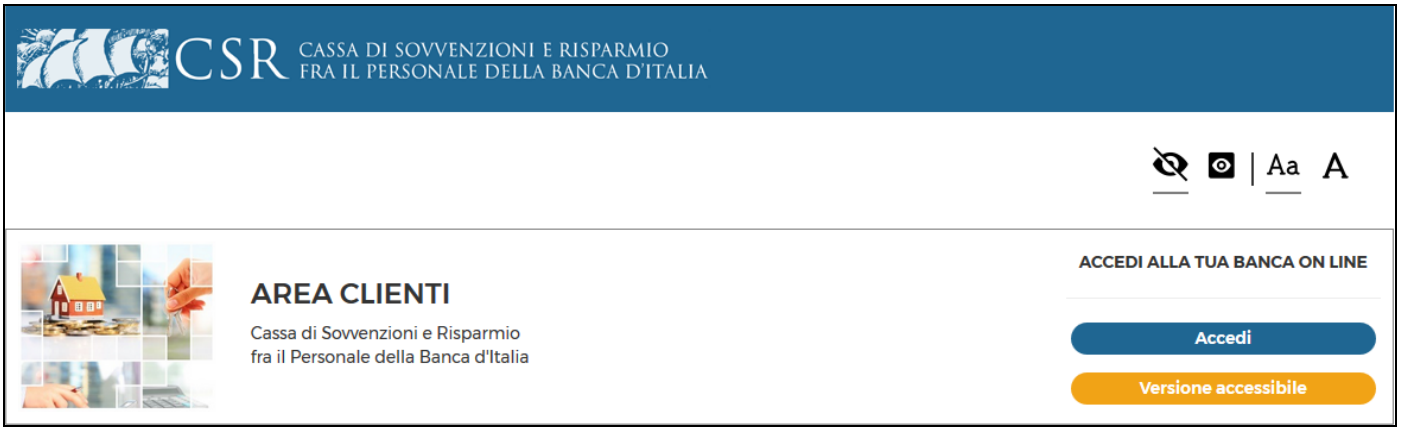
Scegli il tuo PIN personale (può avere da quattro a otto cifre) e premi su PROCEDI:



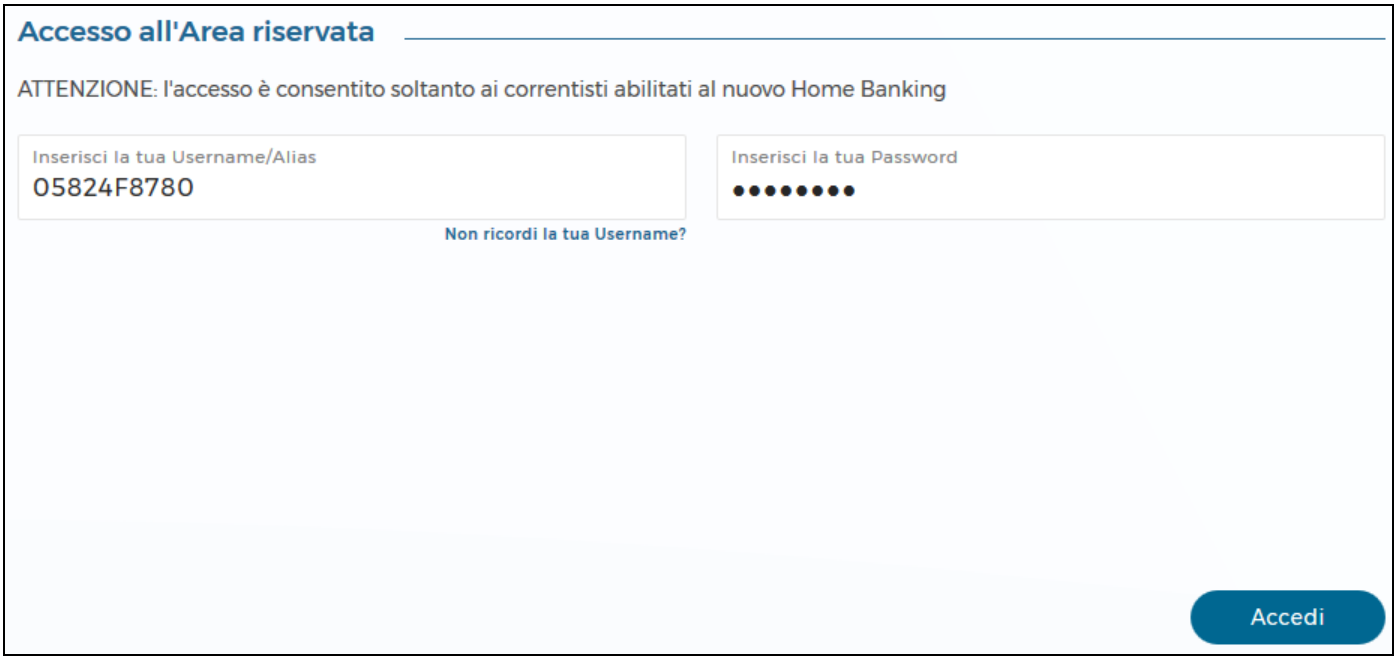
Adesso puoi accedere al tuo home banking, sia da desktop che dall'APP.

2.2 ACCEDERE DA DESKTOP CON IL TOKEN VIRTUALE

Avvia il sito https://www.csrpbi.it e clicca su ACCEDI:



Inserisci la Username e la Password dell'home banking e clicca su ACCEDI:



Comparirà la seguente pagina:

Per ottenere il codice OTP da inserire sul desktop, entra nell'APP e segui queste istruzioni:

Premi su MOBILE TOKEN → Premi su PIN → Inserisci il tuo PIN personale e premi su GENERA OTP

Inserisci il codice OTP sul desktop e clicca su PROCEDI:

Il login è concluso.

2.3 ACCEDERE DA APP CON IL TOKEN VIRTUALE

Entra nell'APP, inserisci la Username e la Password dell'home banking e premi su ACCEDI:

Inserisci il tuo PIN personale, che hai scelto in fase di attivazione del Token virtuale, e premi su PROCEDI:

Il login è concluso.
Ricorda che - solo la prima volta che accedi - devi “certificare” la tua app e scegliere il tuo PIN personale, seguendo le istruzioni al Capitolo 2.1 di questa guida.

3. ACCEDERE CON LA SECURE CALL

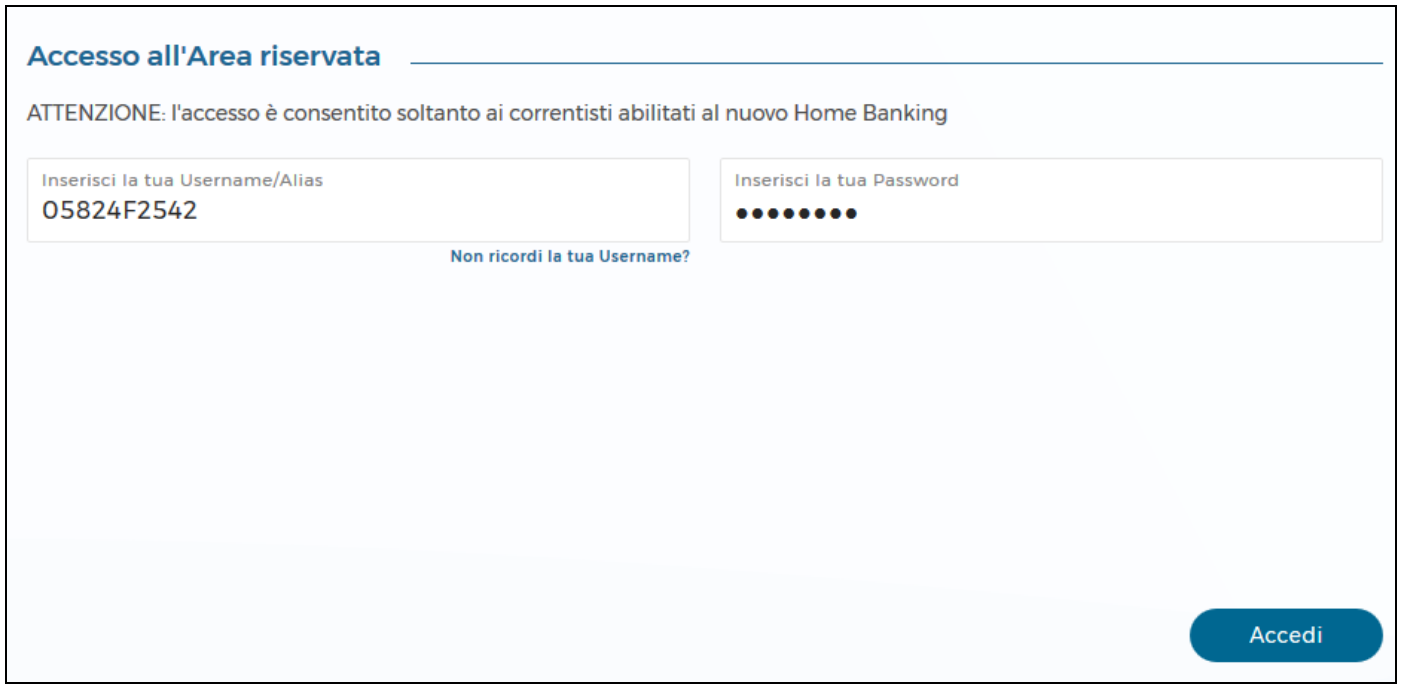
3.1 ATTIVARE LA SECURE CALL

Puoi optare per la Secure call compilando e sottoscrivendo l’apposito modulo - disponibile presso le Rappresentanze e nel sito https://www.csrpbi.it - e presentandolo alla tua Rappresentanza di conto.

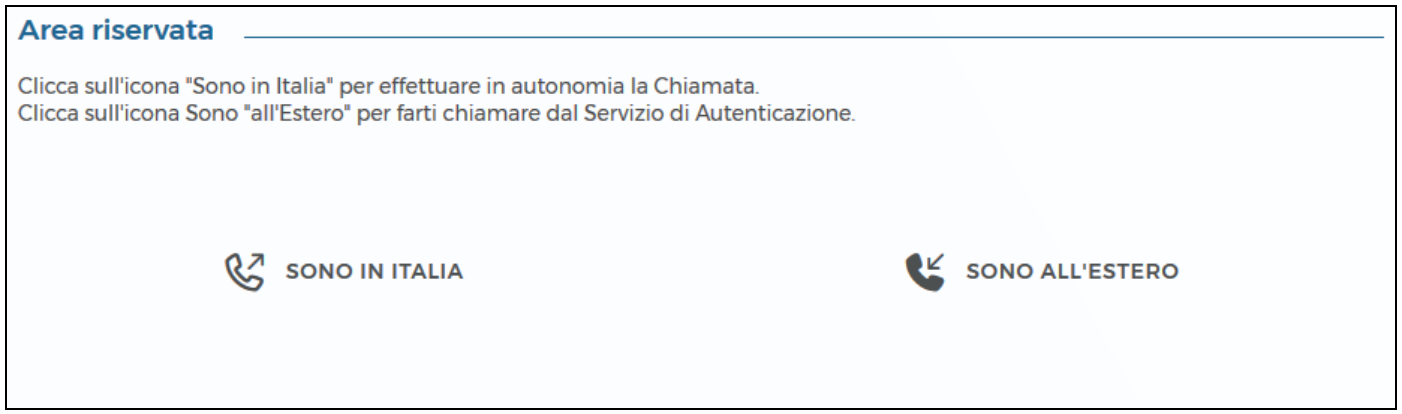
3.2 ACCEDERE DA DESKTOP CON LA SECURE CALL

Avvia il sito https://www.csrpbi.it e clicca su ACCEDI:

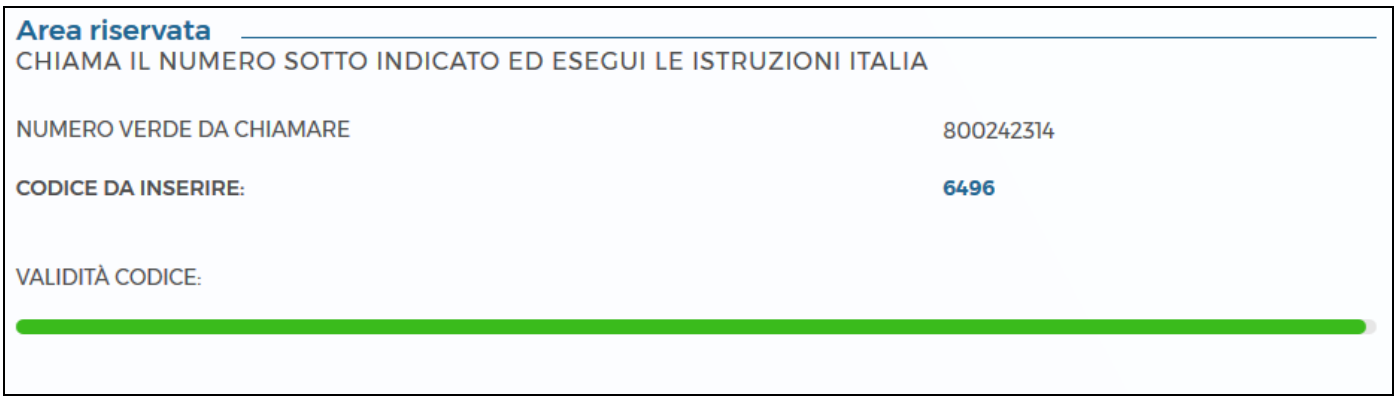
Inserisci la Username e la Password dell’home banking e clicca su ACCEDI:



Clicca su SONO IN ITALIA o SONO ALL'ESTERO:



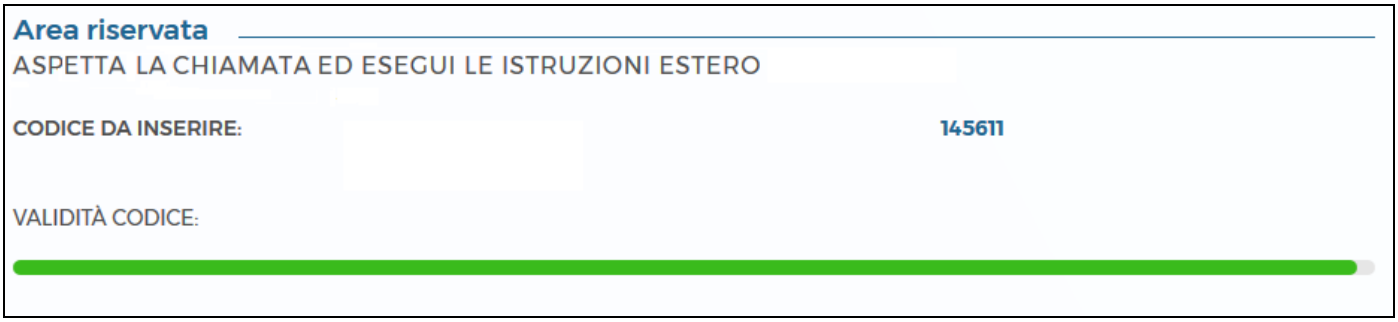
a) Se hai cliccato su SONO IN ITALIA, appariranno sul desktop le seguenti istruzioni:



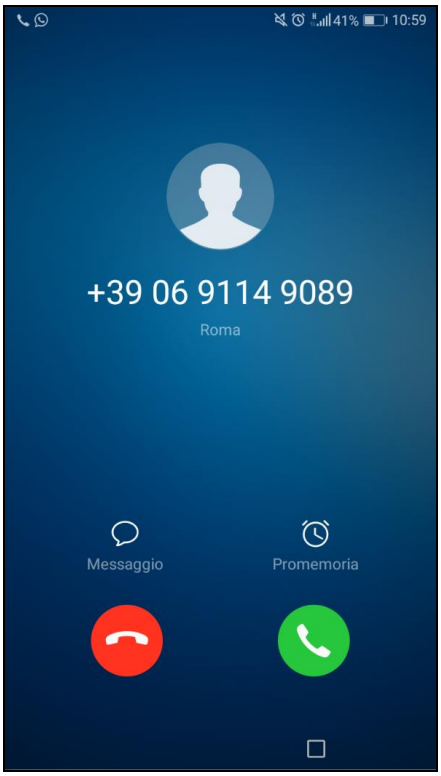
Telefona dal cellulare al numero 800 242314 e digita sulla tastiera del cellulare il codice di quattro cifre che è apparso sul desktop (se hai uno smartphone, per digitare il codice devi

premere il tasto del tuo cellulare che ti consente di visualizzare il tastierino numerico). Il login è concluso.

b) Se hai cliccato su SONO ALL'ESTERO, appariranno sul desktop le seguenti istruzioni:



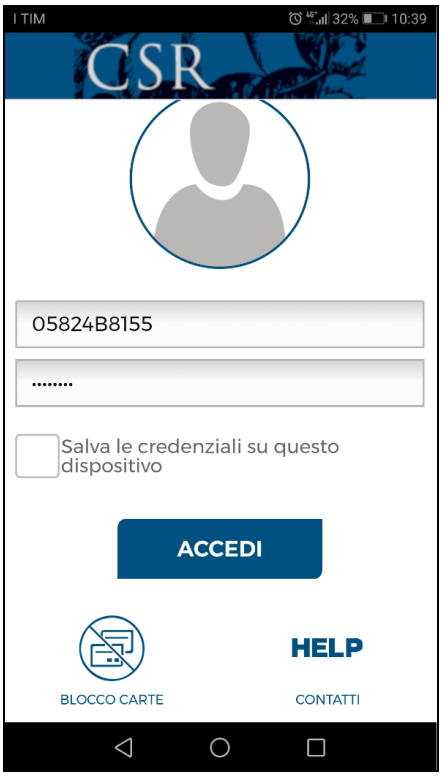
Riceverai una telefonata:



Rispondi e digita sulla tastiera del cellulare il codice di sei cifre che è apparso sul desktop (se hai uno smartphone, per digitare il codice devi premere il tasto del tuo cellulare che ti consente di visualizzare il tastierino numerico). Il login è concluso.

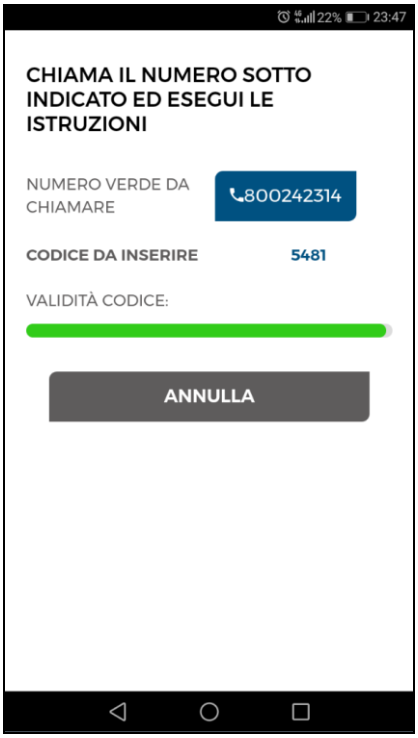
3.3 ACCEDERE DA APP CON LA SECURE CALL

Entra nell'APP, inserisci la Username e la Password dell'home banking e premi su ACCEDI:



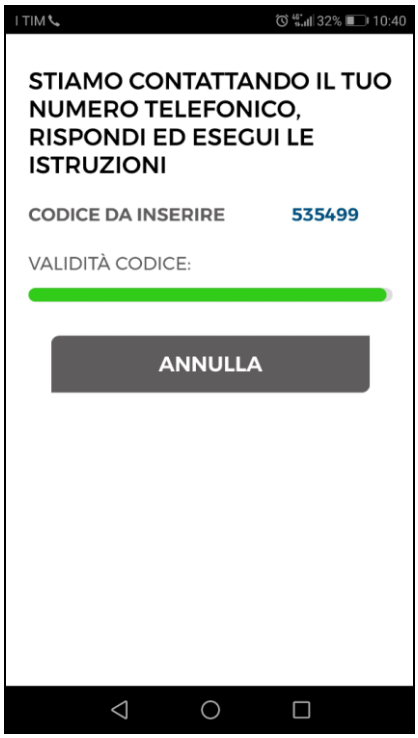
Premi su ITALIA o ESTERO, a seconda di dove ti trovi:

a) Se hai scelto ITALIA, appariranno sullo schermo del cellulare le seguenti istruzioni:

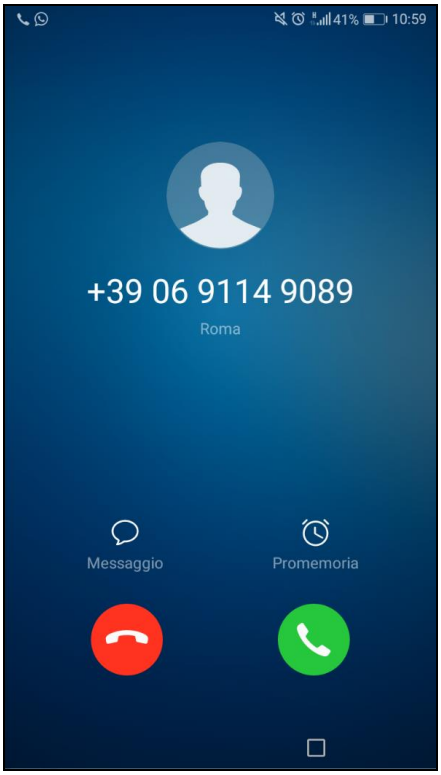


Telefona dal cellulare al numero 800 242314 e digita sulla tastiera del cellulare il codice di quattro cifre che è apparso sullo schermo del cellulare (se hai uno smartphone, per digitare il codice devi premere il tasto del tuo cellulare che ti consente di visualizzare il tastierino numerico). Il login è concluso.

b) Se hai scelto ESTERO, appariranno sullo schermo del cellulare le seguenti istruzioni:



Riceverai una telefonata:

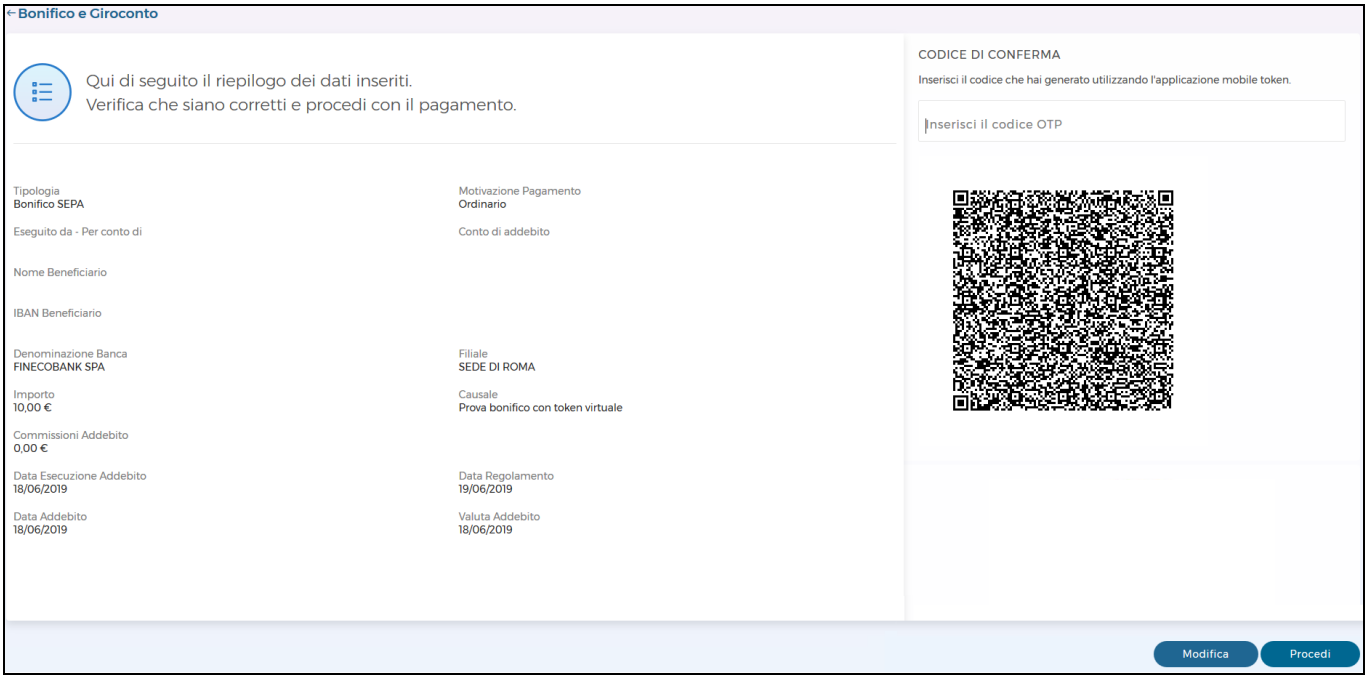


Rispondi e digita sulla tastiera del cellulare il codice di sei cifre che leggi sullo schermo del cellulare (se hai uno smartphone, per digitare il codice devi premere il tasto del tuo cellulare che ti consente di visualizzare il tastierino numerico). Il login è concluso.

4. AUTORIZZARE UN'OPERAZIONE DISPOSITIVA CON IL TOKEN VIRTUALE

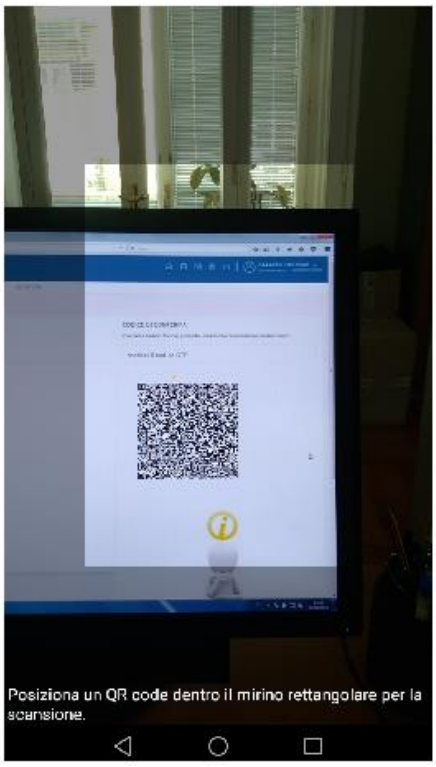
4.1 AUTORIZZARE UN'OPERAZIONE DISPOSITIVA DA DESKTOP CON IL TOKEN VIRTUALE

Inserisci i dati del pagamento, comparirà la seguente pagina:

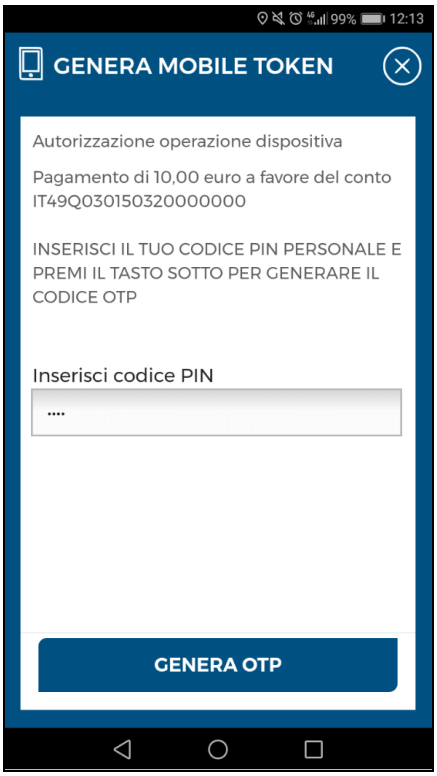


Per ottenere il codice OTP da inserire sul desktop, entra nell'APP e segui queste istruzioni:

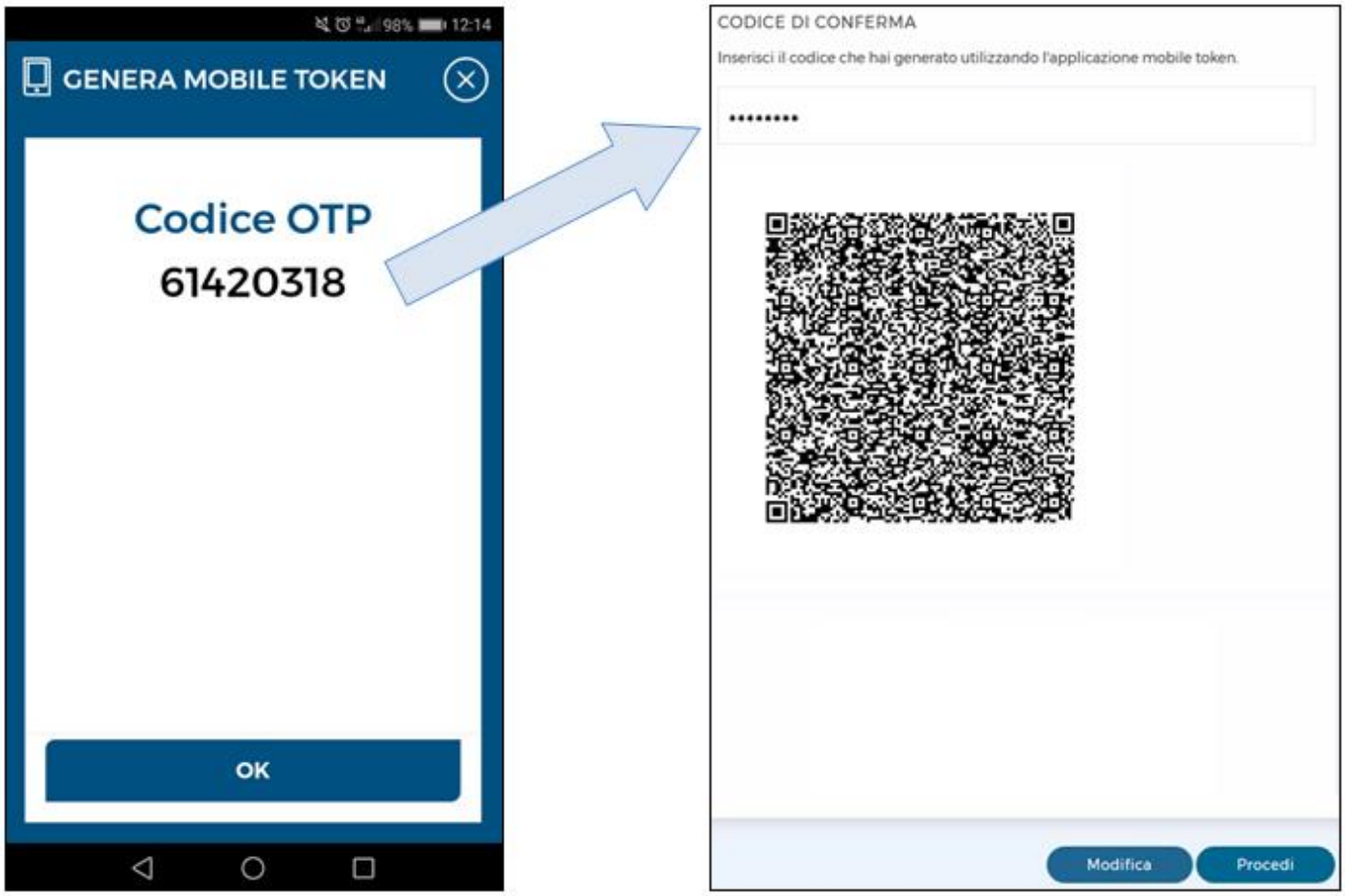
Premi su MOBILE TOKEN → Premi su QRCODE → Inquadra il QRCODE con l'app



L'APP ti proporrà i dati dell'operazione che stai effettuando. Se i dati sono corretti, inserisci il tuo PIN personale, che hai scelto in fase di attivazione del Token virtuale, e premi su GENERA OTP:



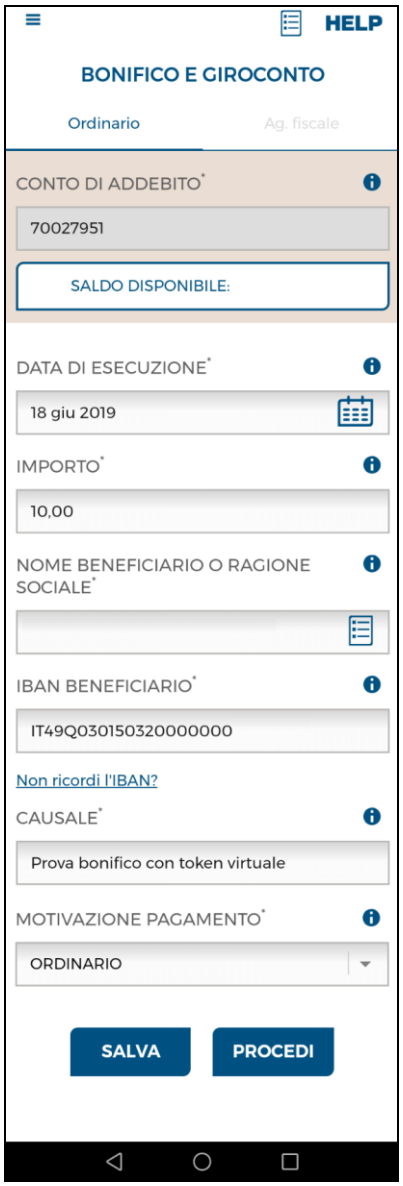
Il Token virtuale genererà un codice OTP. Inseriscilo sul desktop e clicca su PROCEDI:



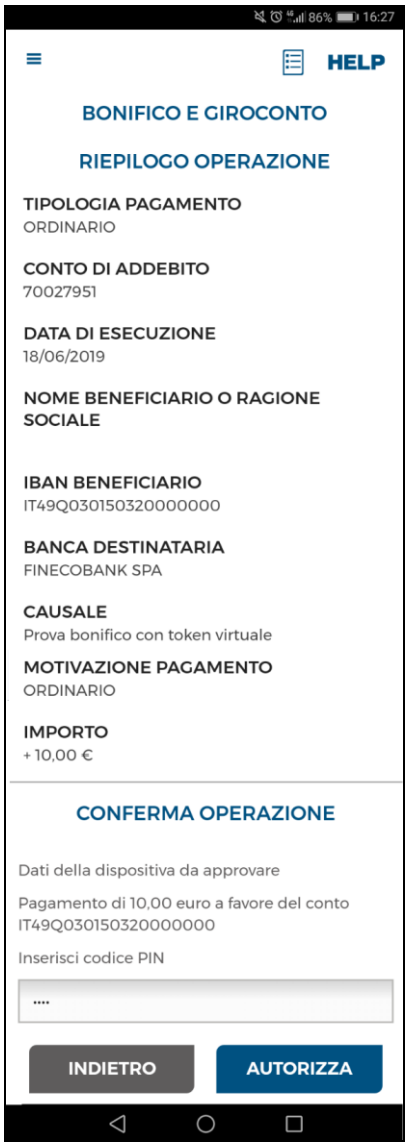
Il pagamento è autorizzato.

4.2 AUTORIZZARE UN'OPERAZIONE DISPOSITIVA DA APP CON IL TOKEN VIRTUALE

Inserisci i dati del pagamento e premi su PROCEDI:



Inserisci il tuo PIN personale, che hai scelto in fase di attivazione del Token virtuale, e premi su AUTORIZZA:

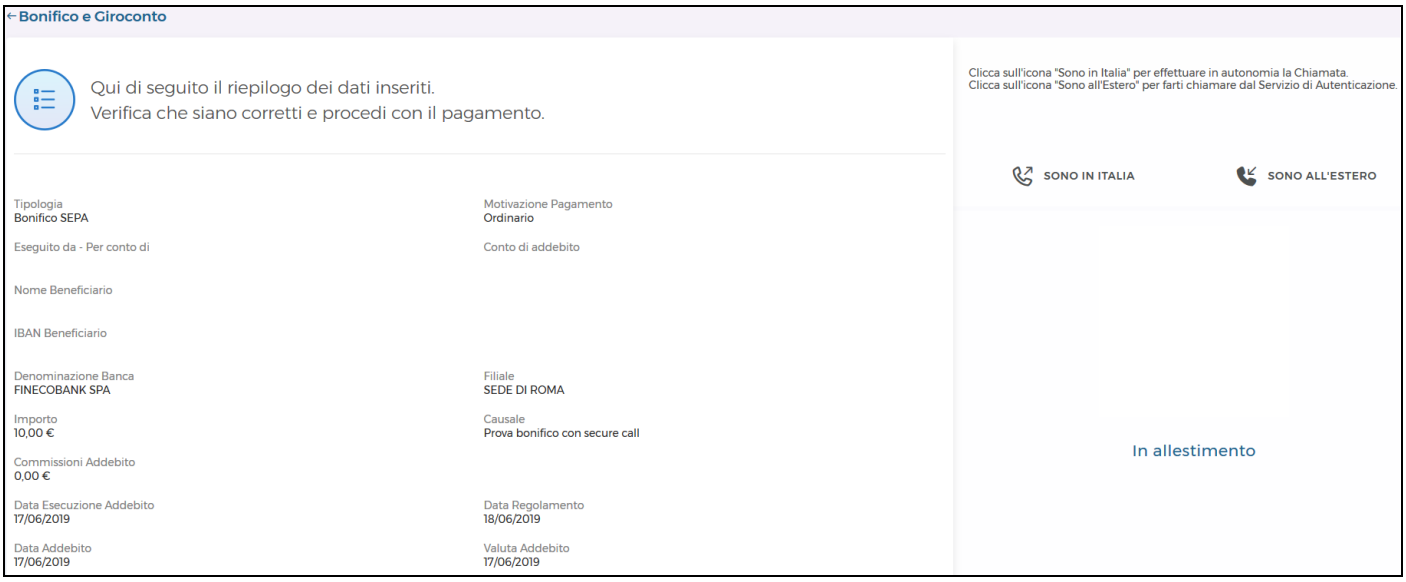


Il pagamento è autorizzato.

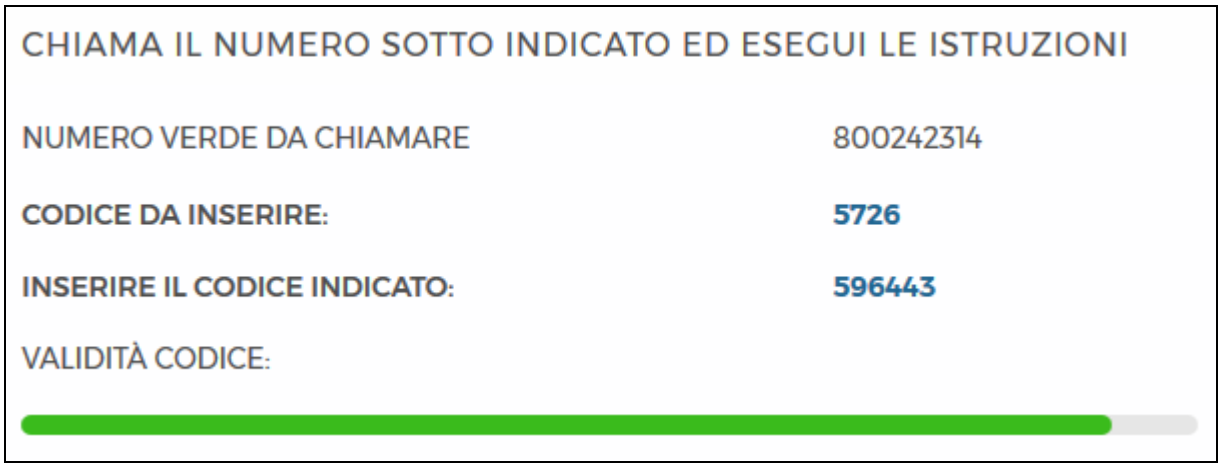
5. AUTORIZZARE UN'OPERAZIONE DISPOSITIVA CON LA SECURE CALL

5.1 AUTORIZZARE UN'OPERAZIONE DISPOSITIVA DA DESKTOP CON LA SECURE CALL

Inserisci i dati del pagamento e clicca su SONO IN ITALIA o SONO ALL'ESTERO:

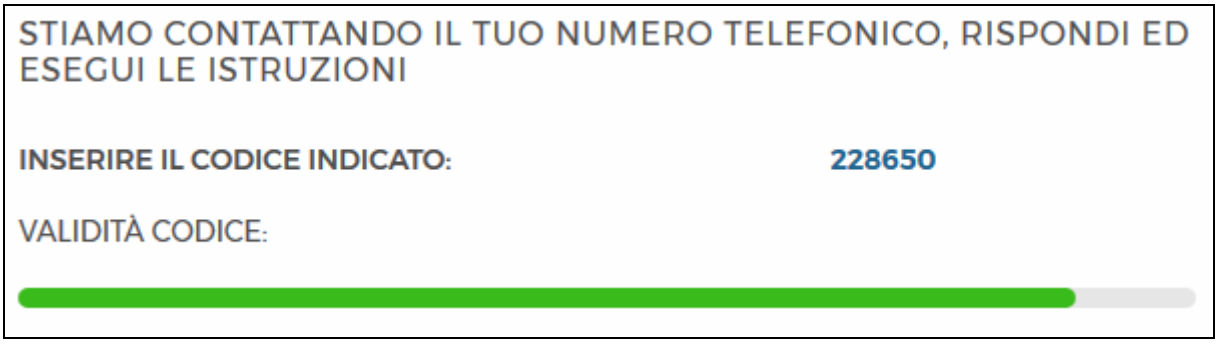


a) Se hai cliccato su SONO IN ITALIA, appariranno sul desktop le seguenti istruzioni:



Telefona dal cellulare al numero 800 242314 e digita sulla tastiera del cellulare il codice di quattro cifre che è apparso sul desktop (se hai uno smartphone, per digitare il codice devi premere il tasto del tuo cellulare che ti consente di visualizzare il tastierino numerico). La voce registrata riepiloga i dati dell'operazione che stai effettuando. Se i dati sono corretti, digita sulla tastiera del cellulare il codice di sei cifre che leggi sul desktop. Il pagamento è autorizzato.

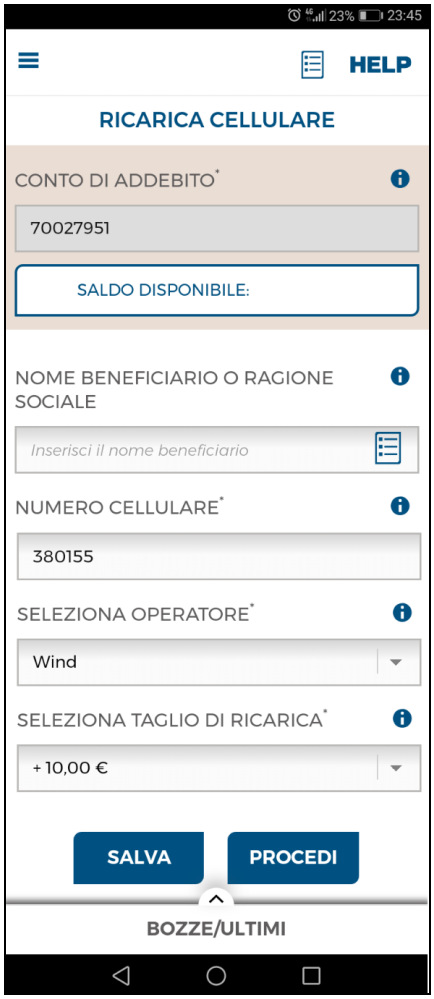
b) Se hai cliccato su SONO ALL'ESTERO, appariranno sul desktop le seguenti istruzioni:



Riceverai una telefonata. La voce registrata riepiloga i dati dell'operazione che stai effettuando. Se i dati sono corretti, digita sulla tastiera del cellulare il codice di sei cifre che leggi sul desktop (se hai uno smartphone, per digitare il codice devi premere il tasto del tuo cellulare che ti consente di visualizzare il tastierino numerico). Il pagamento è autorizzato.

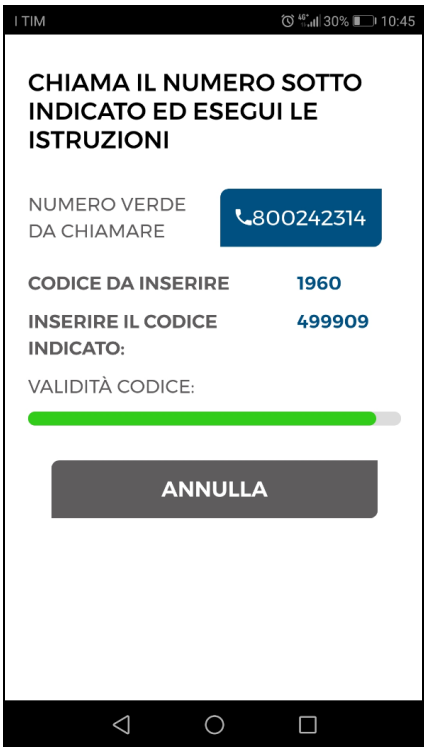
5.2 AUTORIZZARE UN'OPERAZIONE DISPOSITIVA DA APP CON LA SECURE CALL

Inserisci i dati del pagamento e premi su PROCEDI:



Premi su ITALIA o ESTERO, a seconda di dove ti trovi:

a) Se hai scelto ITALIA, appariranno sullo schermo del cellulare le seguenti istruzioni:



Telefona dal cellulare al numero 800 242314 e digita sulla tastiera del cellulare il codice di quattro cifre che leggi sullo schermo del cellulare (se hai uno smartphone, per digitare il codice devi premere il tasto del tuo cellulare che ti consente di visualizzare il tastierino numerico). La voce registrata riepiloga i dati dell'operazione che stai effettuando. Se i dati sono corretti, digita sulla tastiera del cellulare il codice di sei cifre che leggi sullo schermo del cellulare. Il pagamento è autorizzato.

b) Se hai scelto ESTERO, appariranno sullo schermo del cellulare le seguenti istruzioni:

Riceverai una telefonata. La voce registrata riepiloga i dati dell'operazione che stai effettuando. Se i dati sono corretti, digita sulla tastiera del cellulare il codice di sei cifre che leggi sullo schermo del cellulare (se hai uno smartphone, per digitare il codice devi premere il tasto del tuo cellulare che ti consente di visualizzare il tastierino numerico). Il pagamento è autorizzato.

6. CONSIGLI UTILI PER LA SICUREZZA

La sicurezza è il risultato dell'azione combinata della Cassa e del modo in cui utilizzi Internet.

Per garantire la sicurezza della tua operatività, la CSR ha adottato misure che:
- evolvono nel tempo, in funzione delle nuove minacce da contrastare e delle innovazioni della tecnologia a supporto;
- non violano la privacy del cliente;
- non impattano in maniera significativa sull'usabilità del servizio;
- rispettano i requisiti normativi di settore e le best practice del sistema bancario, con particolare

riguardo all'utilizzo di schemi di autenticazione forte (Strong Customer Authentication - SCA).

Come cliente, anche tu hai degli obblighi, che puoi rispettare seguendo le indicazioni che trovi di seguito, tramite le comunicazioni che ti inviamo via email e mantenendoti costantemente informato con quanto verrà pubblicato sul sito della Cassa in tema di sicurezza.

6.1 PROTEGGI LA TUA IDENTITÀ DIGITALE!

L'identità digitale è l'insieme degli elementi che permettono a chi fornisce un servizio di home banking di riconoscerti.

La tua **identità digitale CSR** è composta da:
- **Username**: è il codice di 10 caratteri - invariato nel tempo - che ti è stato fornito quando hai attivato il servizio di home banking;
- **Password iniziale**: è il codice che ti viene assegnato dalla Cassa in fase di attivazione del servizio di home banking; devi modificarla al primo accesso con una password di tua scelta;
- **Password personale**: è la password che scegli al primo accesso e che devi variare periodicamente;
- **Strong Customer Authentication**: è lo standard di autenticazione richiesto dalla Direttiva PSD2 per l'accesso ad un conto online e per l'autorizzazione di pagamenti online. La CSR si è adeguata alla PSD2 dandoti la possibilità di utilizzare, come strumenti di SCA, il Token virtuale integrato nell'app mobile o la Secure call; si tratta di strumenti alternativi tra loro, che hanno sostituito il token fisico utilizzato in precedenza, non più conforme alla normativa di settore;
- **PIN**: è il codice che scegli quando attivi il Token virtuale (se hai attivo, sul tuo contratto telematico, lo schema "Token virtuale"). Può avere da quattro a otto cifre.
- **Numero di cellulare con prefisso italiano** e **indirizzo email**: sono fondamentali per tenere sotto controllo il tuo conto corrente. Ci permettono di contattarti velocemente per informarti o inviarti dati per completare le operazioni, per questo ti chiediamo che siano univoci e sempre aggiornati.

L'identità digitale può essere soggetta a furto e ad utilizzo fraudolento da parte di terzi.
Le frodi informatiche, tra cui le più diffuse sono il phishing ed il crimeware, consistono nell'utilizzare indebitamente informazioni personali di una persona, al fine di identificarsi, in tutto o in parte, nella persona stessa per compiere a suo nome azioni illecite (effettuare disposizioni bancarie oppure per ottenere credito tramite false credenziali).

ATTENZIONE: se pensi di essere stato oggetto di una frode informatica, contatta immediatamente il servizio di assistenza clienti al numero 800 183 447, che si attiverà subito per bloccare la tua utenza.

6.2 COS'È IL PHISHING

Il **phishing** è una frode informatica attuata tramite l'invio di email, SMS o falsi annunci pubblicitari presenti sul web che portano l'utente su pagine in cui viene richiesto l'inserimento di informazioni

riservate. In genere sono pagine composte utilizzando il logo, il nome e il layout tipico dell'azienda imitata, come ad esempio una banca oppure una società emittente carte di credito. Le comunicazioni di phishing spesso sono generiche, non si rivolgono specificatamente a te e contengono errori ed imprecisioni.

ATTENZIONE: La Cassa non richiede mai informazioni personali via email, telefono o SMS.

6.3 COS'È IL CRIMEWARE

Il **crimeware** è una frode informatica attuata diffondendo, presso postazioni non adeguatamente protette, un codice malevolo (malware) in grado di rubare informazioni riservate del cliente e di consentire il controllo da remoto della postazione contaminata. Di solito, la diffusione dei malware avviene tramite un supporto fisico (come un CD-Rom o una Pen Drive), gli allegati contenuti nelle email, scaricando dati e programmi da Internet o navigando su siti non sicuri.

6.4 UTILIZZARE IN SICUREZZA L'HOME BANKING

- Conserva tutti i dati che compongono la tua identità digitale con la **massima riservatezza**: non memorizzare mai la tua password e/o il tuo PIN sul cellulare, sul computer oppure sul browser; quando scegli la Password personale e il PIN componili in maniera non banale e difficilmente riconducibile ad informazioni che riguardano te o la tua famiglia.
- Non usare password o PIN già utilizzate per altri servizi; **modifica frequentemente la password** di accesso al tuo home banking.
- **Non divulgare sui social network informazioni che riguardano la tua identità** (data o luogo di nascita, indirizzo, numero di telefono).
- Utilizza sul tuo PC, tablet o smartphone **antivirus** e antispyware, tenendoli sempre aggiornati.
- **Non accedere all'home banking da computer pubblici o utilizzando reti Wi-Fi non sicure.** Utilizzare computer in Internet Café, biblioteche, università o luoghi simili è rischioso perché potrebbero contenere malware in grado di registrare ciò che stai digitando; se utilizzi una rete non sicura i tuoi dati potrebbero essere facilmente intercettati.
- Ricordati sempre di **mantenere aggiornati il tuo numero di telefono e il tuo indirizzo email**: ti permetterà di operare in completa sicurezza e ci darà la possibilità di contattarti tempestivamente in caso di necessità.
- Quando hai terminato di utilizzare l'home banking effettua sempre il **logout** per disconnettere la sessione.

7. BLOCCARE L'UTENZA DI HOME BANKING

In caso di smarrimento o furto del telefono cellulare e/o delle credenziali di accesso, l'utente deve contattare prontamente il Servizio di assistenza clienti al numero **800 183 447** per il blocco dell'account e delle disposizioni e deve darne quanto prima comunicazione alla Cassa.

8. SBLOCCARE L'UTENZA DI HOME BANKING

8.1 COSA FARE SE LA TUA UTENZA È BLOCCATA

Se la tua utenza di home banking è bloccata, chiama il Servizio di assistenza clienti al numero **800 183 447** per chiederne lo sblocco. In particolare, chiedi:
- lo sblocco della Password personale, se ricordi l'ultima Password che hai impostato;
- il reset della Password, se non ricordi l'ultima Password che hai impostato. In questo caso dovrai effettuare il successivo accesso all'home banking utilizzando la Password iniziale; se non ricordi neanche la Password iniziale, contatta la tua Rappresentanza;
- il reset del PIN personale, se non ricordi il tuo PIN personale. In questo caso, al successivo accesso all'app della CSR, dovrai impostare un nuovo PIN personale;
- lo sblocco dell'utenza, se hai sbagliato l'inserimento dei codici per l'utilizzo della Secure call.

8.2 COSA FARE SE CAMBI CELLULARE

- Se cambi il **numero di telefono** cellulare, comunica il nuovo numero alla tua Rappresentanza.
- Se hai scelto il Token virtuale e cambi lo **smartphone**, il Token virtuale deve essere reinstallato (perché è associato ad uno specifico dispositivo telefonico per motivi di sicurezza); chiama il Servizio di assistenza clienti al numero **800 183 447** e chiedi la disinstallazione del Token virtuale; dopodiché installa il Token virtuale sul nuovo cellulare seguendo le istruzioni al Capitolo 2.1 di questa guida.
- Se hai scelto la Secure call e cambi il cellulare o lo smartphone (ma non il numero di telefono), non devi fare niente.