SERVIZIO *AGENZI@BPB*

GRUPPO BANCA POPOLARE DI BARI

agenzi@bpb net banking Privati

ISTRUZIONI OPERATIVE PER LA REGISTRAZIONE E L'ACCESSO AL SERVIZIO

PROFILI CON FUNZIONI INFORMATIVE E DISPOSITIVE

PROFILI CON TOKEN FISICO (CHIAVETTA)

PROFILI CON MOBILE TOKEN

NOTA APPROFONDIMENTO PROFILI CON SECURE CALL

ISTRUZIONI PER UTILIZZARE LA FUNZIONE "*AUTORESET*" (SBLOCCO *PASSWORD ONLINE*)

PROFILI CON TOKEN FISICO (CHIAVETTA)

PRIMO ACCESSO - REGISTRAZIONE AL SERVIZIO

Si descrivono, con immagini esemplificative, le fasi da seguire per effettuare correttamente l'autenticazione e l'accesso al portale.

- Accedere al sito **www.agenziabpb.it**.
- N.B. è possibile accedere al sito **www.agenziabpb.it** anche dal sito internet **www.popolarebari.it** cliccando sull'icona area clienti e successivamente sul tasto "privati"

- Nel campo **La tua Banca** selezionare la propria banca di appartenenza fra Banca Popolare di Bari e Cassa di Risparmio di Orvieto;
- Nel campo **Username** inserire i 10 caratteri del codice utente
- Nel campo **Password** inserire la password alfanumerica ricevuta dalla Banca (password iniziale).
- Premere il tasto **Accedi**.
- Conservare con cura, separatamente, lo **Username** e la **Password Iniziale** (*).

(*) Il **Codice Utente (Username)** assegnato dalla Banca al momento dell'attivazione del contratto resta immutato e deve essere utilizzato per ogni accesso al servizio. La **Password Iniziale** assegnata dalla Banca al momento dell'attivazione del contratto deve essere cambiata al primo accesso al portale, per motivi di sicurezza; deve essere comunque conservata con cura per ogni eventuale futuro utilizzo.

- Inserire il **numero** visualizzato nel **display della chiavetta OTP**.
- Premere il tasto **Accedi**.

CAMBIO PASSWORD INIZIALE

Per motivi di sicurezza, l'utente deve cambiare la password iniziale ricevuta dalla banca e definirne una nuova.
Il cambio della password è comunque richiesto ogni 180 giorni.

- Nel campo **Vecchia Password** digitare la password iniziale ricevuta dalla Banca.
- Definire e digitare nel campo **Nuova Password** un **codice alfanumerico** (numeri e lettere, minuscole e/o maiuscole) **compreso tra 8 e 30 caratteri**.
- Digitare con attenzione nel campo **Ripeti password** la Password scelta ed inserita nel campo **Nuova Password**.
- Premere il tasto **Modifica**.

Terminata la modifica della *password* iniziale viene visualizzata la *home page* del portale.

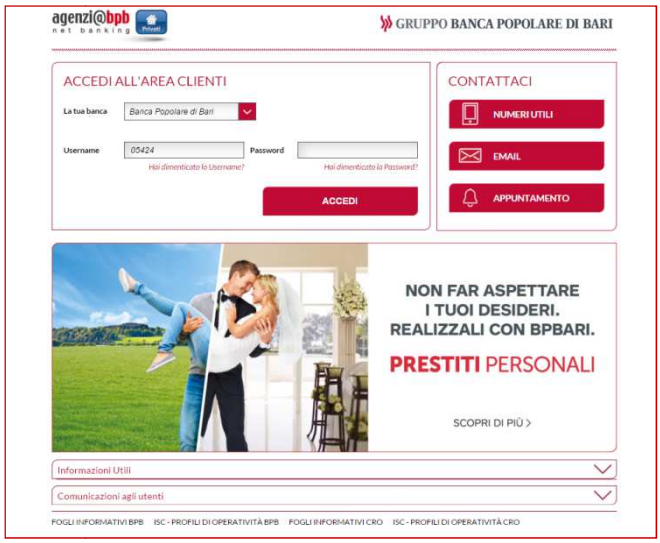
Per utilizzare il servizio occorre selezionare le funzioni di interesse (pagamenti, my account, ecc.).

Per informazioni sulle funzioni disponibili e per un supporto nell'operatività, è possibile consultare l'*Help Online*, la guida alla navigazione nel portale *agenzi@bpb*.
Per ogni funzione, il servizio di *Help Online* propone, mediante finestre di dialogo, una sintetica definizione della funzione e una specifica guida all'utilizzo della stessa, con la descrizione delle modalità di compilazione dei campi.
La consultazione dell'*Help Online* può avvenire:

- da **Servizi > Servizi accessori > Help**, per una visualizzazione completa dell'Help disponibile sul portale;
- dal comando in alto a destra (?) disponibile in ogni area o sezione di navigazione, per avere informazioni sulle singole funzioni che l'utente sta utilizzando.

ACCESSI SUCCESSIVI – UTILIZZO DEL SERVIZIO

- Accedere al sito **www.agenziabpb.it**.
- N.B. è possibile accedere al sito www.agenziabpb.it anche dal sito internet www.popolarebari.it cliccando sull'icona area clienti e successivamente sul tasto "privati"



- Inserire le credenziali in uso come specificato nel paragrafo precedente (**La tua Banca; Username** e **Password**).
- Premere il tasto **Accedi**.

- Inserire il **numero** visualizzato nel **display della chiavetta OTP**.
- Premere il tasto **Accedi**.

Terminata l'autenticazione con l'inserimento delle credenziali viene visualizzata la *home page* del portale.

Per utilizzare il servizio occorre selezionare le funzioni di interesse (pagamenti, my account, ecc.).

PROFILI CON MOBILE TOKEN

PRIMO ACCESSO - REGISTRAZIONE AL SERVIZIO

Per poter utilizzare il mobile token è necessario essere in possesso di uno smartphone IOS o Android.

Effettuare il *download* dell'applicazione **agenzi@bpb** dagli *store* Android o IOS dipendentemente dallo smartphone utilizzato.

Si descrivono, con immagini esemplificative, le fasi da seguire per la prima registrazione al servizio **agenzi@bpb** attraverso la App, qualora il cliente intenda effettuare il primo accesso attraverso il Mobile Banking.

Si tratta di un'ipotesi consigliata per i clienti che hanno richiesto il mobile token in fase di contrattualizzazione del servizio agenzi@bpb e NON abbiano già effettuato la prima autenticazione tramite il portale web di internet banking (www.agenziabpb.it).

Aprire l'applicazione sul proprio smartphone.

CAMPI CREDENZIALI

Schermata home page della app

Campi credenziali

Pulsante per generazione codici OTP mobile token

- Nel campo **Codice Utente** inserire il codice di 10 caratteri ricevuto dalla Banca
- Nel campo **Password** inserire la password alfanumerica ricevuta dalla Banca (password iniziale).
- Premere il tasto **Accedi**.
- Il sistema invia automaticamente all'indirizzo *mail* del cliente una *email* per l'installazione del *mobile token* sullo *smartphone*
- Conservare con cura, separatamente, il **Codice Utente** e la **Password Iniziale** (*).

(*) Il **Codice Utente** assegnato dalla Banca al momento dell'attivazione del contratto resta immutato e deve essere utilizzato per ogni accesso al servizio. La **Password Iniziale** assegnata dalla Banca al momento dell'attivazione del contratto deve essere cambiata al primo accesso al portale, per motivi di sicurezza; deve essere comunque conservata con cura per essere riutilizzata in caso di eventuale blocco dell'utenza e successivo ripristino.

E TOKEN

token

denziali

aggio è lo

Aprire la mail ricevuta sullo stesso dispositivo su cui si intende installare il *mobile token*

Seguire le istruzioni di installazione.

Installazione automatica

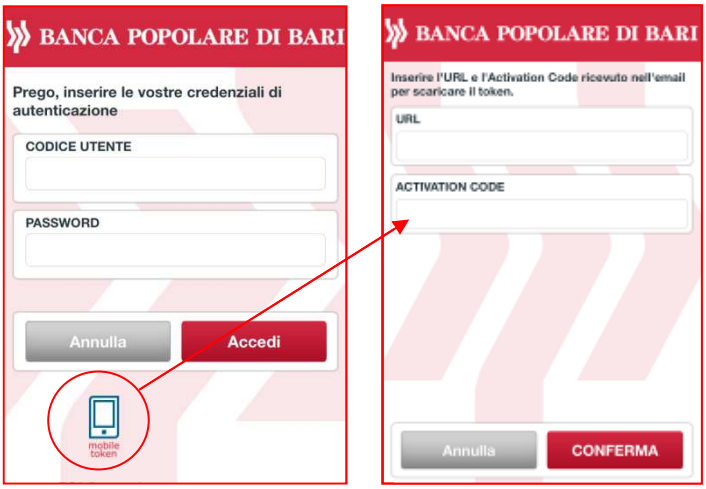
Cliccare sul link relativo al proprio sistema operativo (IOS/Android); il mobile token verrà installato sul dispositivo ed un apposito messaggio informerà l'utente dell'avvenuta installazione.

Installazione manuale

Qualora non funzionasse il *link*, il cliente dovrà utilizzare i dati indicati nella parte inferiore della mail, ovvero:

URL
Activation Code

Per poter inserire i dati sopra indicati il cliente dovrà aprire la funzionalità *mobile token* dalla home page della app e riportarli nei campi specifici.



IANUALE MOBILE TOKEN

on Code da copiare dalla mail di
re negli appositi campi

Installato con successo il mobile token il cliente dovrà ripetere l'accesso dall'app.

MPI CREDENZIALI

hermata home page della app

mpi credenziali

lsante per generazione codici OTP mobile token

- Nel campo **Codice Utente** inserire il codice di 10 caratteri ricevuto dalla Banca
- Nel campo **Password** inserire la password alfanumerica ricevuta dalla Banca (password iniziale).
- Premere il tasto **Accedi**.

MPOSTAZIONE PIN DISPOSITIVO

er poter operare online il cliente deve impostare un PIN
i 4 cifre che gli verrà richiesto dall'app per la
enerazione dei codici dispositivi del mobile token

- Nel campo **Nuovo Pin** digitare un codice di 4 cifre.
- Nel campo **Verifica Nuovo Pin** ridigitare il codice immesso prima
- Premere il tasto **Accedi**.

N.B. E' fondamentale ricordare il codice Pin in quanto è necessario per l'autorizzazione di tutte le operazioni dispositive sia da pc che da app mobile.

CAMBIO CREDENZIALI

vi di sicurezza, l'utente deve cambiare la password
icevuta dalla banca e definirne una nuova.
della password è comunque richiesto ogni 180 giorni.

- Nel campo **Vecchia Password** digitare la password iniziale ricevuta dalla Banca.
- Definire e digitare nel campo **Password** un codice alfanumerico (numeri e lettere, minuscole e/o maiuscole) **compreso tra 8 e 30 caratteri**.
- Digitare con attenzione nel campo **Conferma password** la Password scelta ed inserita nel campo **Password**.
- Premere il tasto **Accedi**.

ACCESSI SUCCESSIVI – UTILIZZO DEL SERVIZIO

- Accedere al sito **www.agenziabpb.it**.

- Inserire le credenziali in uso come specificato nel paragrafo precedente (**La tua Banca; Username** e **Password**).
- Premere il tasto **Accedi**.

Generare sulla app un **codice OTP** con il mobile token (vedi paragrafo "**generare un codice OTP con il mobile token**")

Inserire il **codice OTP passcode** visualizzato sul **display dello smartphone.**

- Premere il tasto **Accedi**.

Terminata l'autenticazione con l'inserimento delle credenziali viene visualizzata la *home page* del portale.

Per utilizzare il servizio occorre selezionare le funzioni di interesse (pagamenti, my account, ecc.).

GENERARE UN CODICE OTP CON IL MOBILE TOKEN

Di seguito vengono descritti i passaggi con le relative schermate utili per poter generare un codice OTP dal mobile token.

Aprire l'applicazione sul proprio smartphone.

1

Accedere alla funzionalità mobile token dall'icona in basso a sinistra 

2

Inserire il pin di 4 cifre impostato al primo accesso e premere OK.

3

Il codice generato che dura 30 secondi è il codice OTP che deve essere usato quando richiesto nelle operazioni di internet banking su pc.

RESET MOBILE TOKEN/RESET PIN

In caso di smarrimento dello smartphone o nel caso in cui il cliente non ricordi più il PIN personale bisognerà procedere ad un reset del mobile token o del solo PIN.
Per poter effettuare il reset del mobile token o del PIN il cliente deve rivolgersi al numero verde della banca 800.005.444.

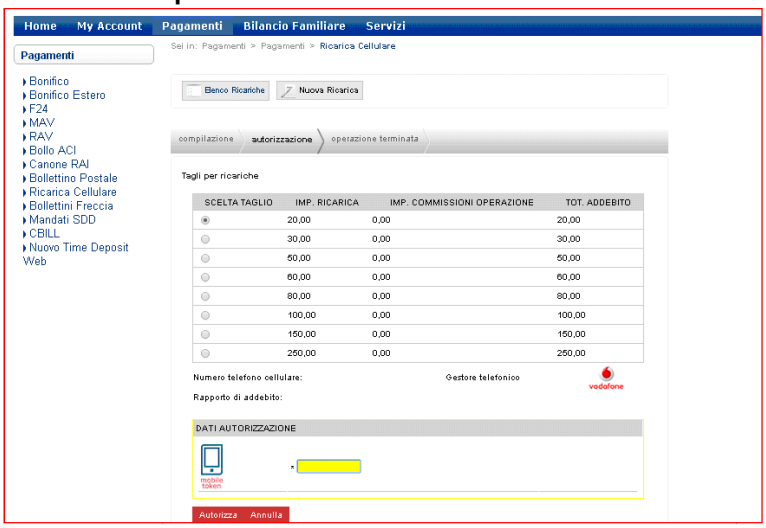
N.B. Il reset del PIN non comporta necessariamente il reset del mobile token e viceversa; quindi il cliente che richiede il solo reset del mobile token potrà continuare ad utilizzare il proprio PIN personale.

AUTORIZZARE UN'OPERAZIONE DISPOSITIVA CON IL MOBILE TOKEN

Internet banking (PC)

Nel caso di operazioni dispositive (es. bonifico, ricarica cellulare ecc) eseguite da PC sull'internet banking agenzi@bpb, nella schermata finale dell'operazione viene richiesto al cliente di inserire un codice OTP generato con il mobile token.

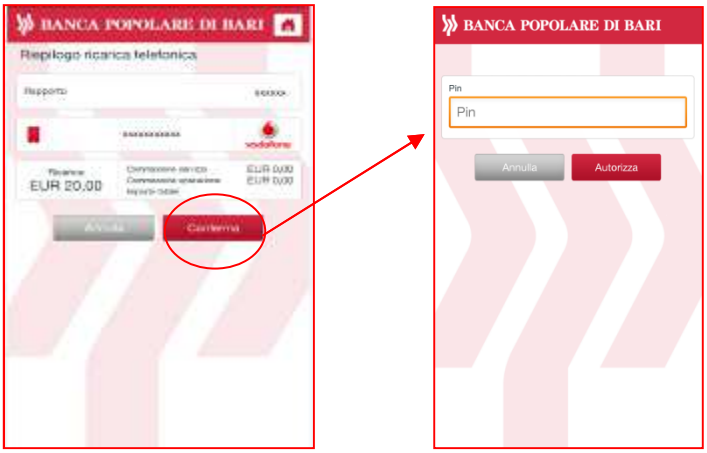
Esempio schermata di conferma operazione ricarica cellulare



Il cliente deve generare un codice OTP sul proprio smartphone (come descritto nell'apposito paragrafo pag.13) e digitarlo nel campo dedicato 

Mobile banking su app

Nel caso di operazioni dispositive (es. bonifico, ricarica cellulare ecc) eseguite su smartphone mediante l'app, nella fase finale dell'operazione, quando richiesto, il cliente dovrà inserire il solo PIN di 4 cifre.
L'applicazione del mobile token è integrata nella app di banking e quindi ad ogni disposizione da app il cliente dovrà inserire il solo PIN per autorizzare l'operazione perché la app genera la OTP automaticamente.



N'OPERAZIONE DISPOSITIVA

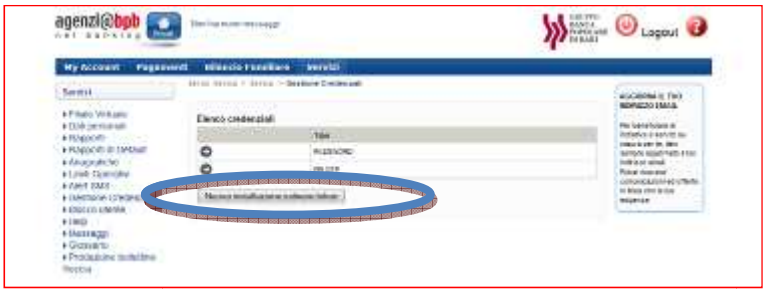
a cellulare da app, dopo aver inserito
ati della ricarica e premendo il tasto
inserire il solo PIN per autorizzare

RIEMISSIONE MOBILE TOKEN

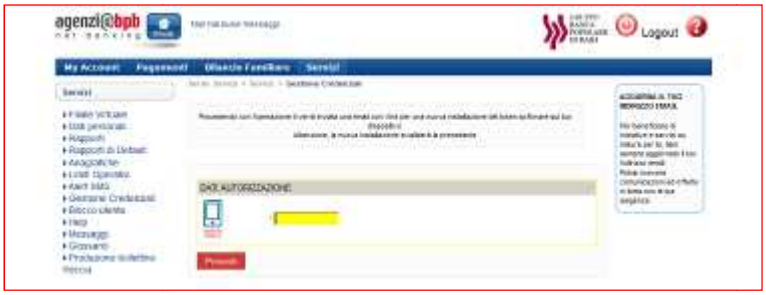
Nel caso in cui il cliente volesse utilizzare il mobile token su un nuovo dispositivo è necessario procedere con la funzione di remissione del mobile token, che dovrà essere installato sul nuovo dispositivo.

Tramite l'apposita funzionalità di internet banking "Nuova installazione mobile token" il cliente può in autonomia richiedere remissione del software token.

- Effettuare il login in agenzi@bpb



- Selezionare dalle voci di menu in alto **Servizi**
- Selezionare sul menu di sinista la funzione **Gestione Credenziali**
- Premere il tasto **Nuova installazione software token**

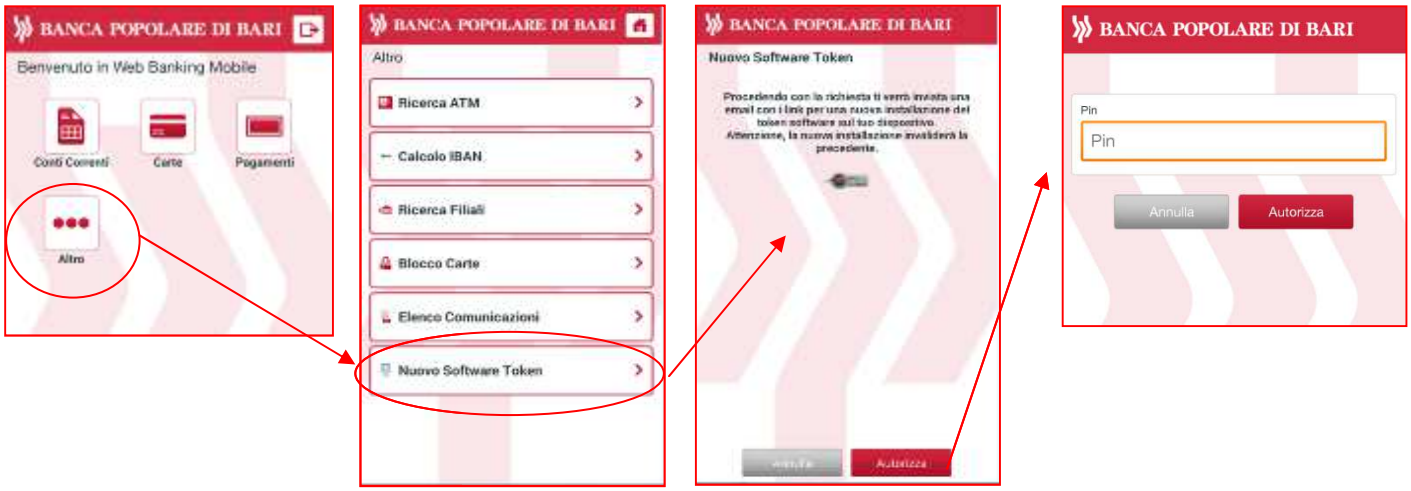


- Autorizzare l'operazione inserendo un codice OTP generato dall'app nell'apposito campo (come descritto nell'apposito paragrafo pag.13)
- Premere il tasto **Procedi**

Il cliente riceve la mail di attivazione e può procedere con l'installazione come descritto nell'apposito paragrafo.

N.B. l'attivazione di un nuovo mobile token invalida la precedente. Il cliente può avere a disposizione un solo mobile token su un solo dispositivo.

E' possibile richiedere la riemissione del mobile token anche da smartphone tramite la funzionalità dell'app "nuovo software token" del menu "altro".



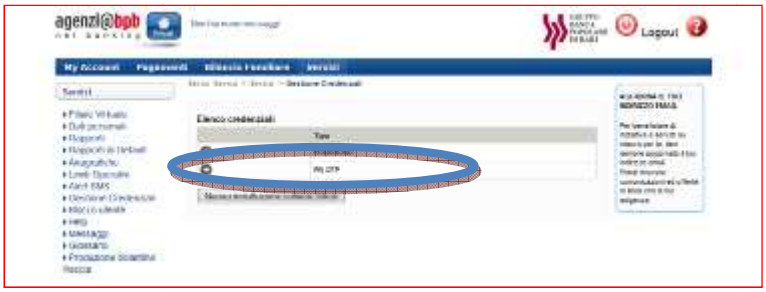
MODIFICA DEL PIN DEL MOBILE TOKEN

Tramite l'apposita funzionalità di internet banking "Gestione Credenziali>PIN OTP" il cliente può in autonomia modificare il PIN personale impostato in fase di attivazione del mobile token.

Questa funzionalità è accessibile solo da PC sull'internet banking Agenzi@bpb.

N.B. il nuovo PIN deve essere diverso dagli ultimi tre impostati dal cliente

- Effettuare il login in agenzi@bpb



- Selezionare dalle voci di menu in alto **Servizi**
- Selezionare sul menu di sinistra la funzione **Gestione Credenziali**
- Premere il tasto → in corrispondenza della voce PIN OTP

- Digitare il nuovo PIN di 4 cifre che si intende impostare nel campo **Nuovo PIN OTP**
- Ridigitare per conferma il nuovo PIN nel campo **Ripeti PIN OTP**
- Autorizzare l'operazione inserendo un codice OTP generato dall'app nell'apposito campo (come descritto nell'apposito paragrafo)
- Premere il tasto **Modifica**

Il nuovo Pin è stato salvato e il cliente dovrà utilizzarlo per tutti i successivi utilizzi del mobile token.

NOTA APPROFONDIEMENTO PROFILI CON SECURE CALL

Per i soli profili dotati di **secure call**, il servizio di conferma delle operazioni dispositive mediante telefonata ad una numerazione speciale, valgono le regole operative approfondite di seguito.
Si specifica che il servizio è valido esclusivamente per i clienti Tercas e Caripe che ne sono già in possesso.

Login

Per effettuare l'accesso ad agenzi@bpb il cliente deve inserire nella maschera di login i seguenti dati:

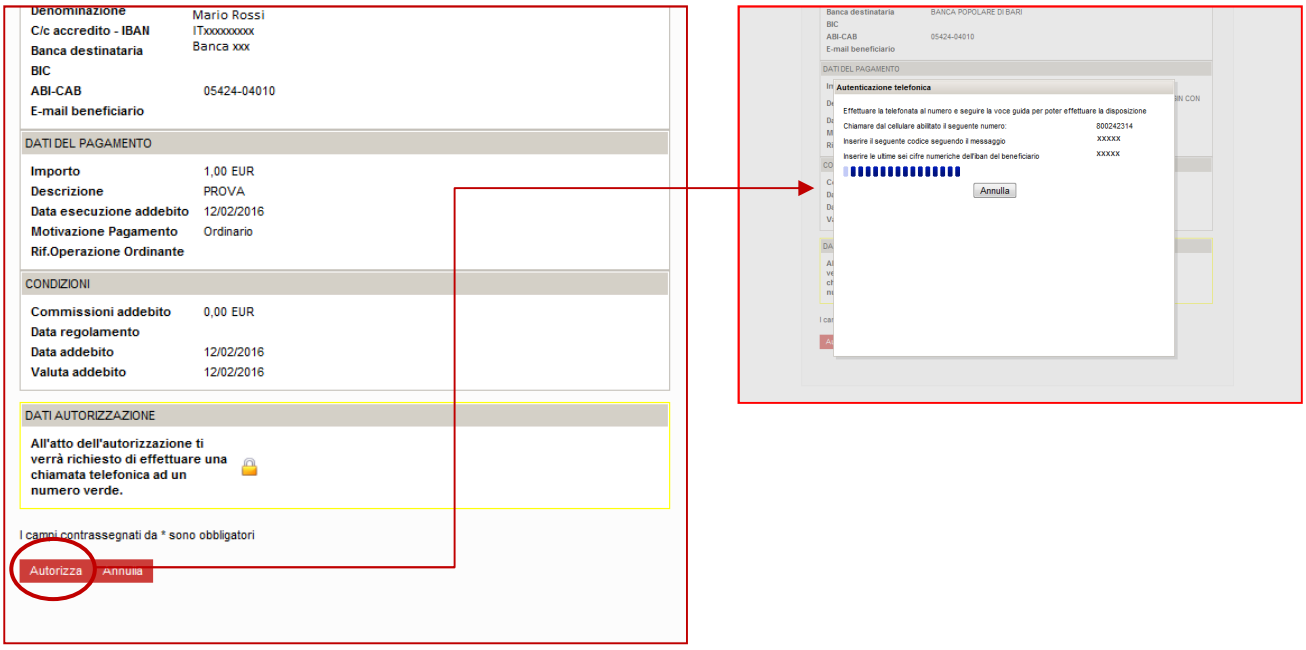
- **Username** di 10 caratteri (che inizia con 05424) o alternativamente il **codice ID** utilizzato per gli accessi al precedente home banking;
- Password personale;

Non verrà richiesto l'inserimento di nessuna altra credenziale per accedere in modalità informativa al proprio home banking.

Conferma delle operazioni dispositive

Per poter confermare le operazioni dispositive (es. bonifico ordinario) a valle della compilazione di tutti i dati necessari per inviare la disposizione, il cliente deve:

- Cliccare su autorizza;
- Chiamare dal proprio telefono cellulare il numero speciale indicato e seguire le istruzioni della voce guida.



ERRORI NELL'ACCESSO AL SERVIZIO E IPOTESI DI BLOCCO DELL'UTENZA

Nell'accesso al servizio di agenzi@bpb possono verificarsi errori nell'inserimento delle credenziali (codice utente, password, token) o di altri codici richiesti di volta in volta dalla procedura (codice CAPTCHA, ecc.).

Quando il numero massimo di errori consentiti non viene superato, l'utente inserisce il valore corretto, digita il codice CAPTCHA e procede regolarmente con l'accesso al servizio, senza che intervenga un blocco (cfr. "ESEMPIO DI ERRORE CHE NON GENERA IL BLOCCO DELL'UTENZA" di seguito riportato).

Il CAPTCHA è una sequenza di lettere e numeri, generata automaticamente e in modo casuale, che appare distorta o offuscata sullo schermo. Nel caso in cui il codice risulti illeggibile all'utente, è possibile generarne un altro con il comando "Cambia CAPTCHA".

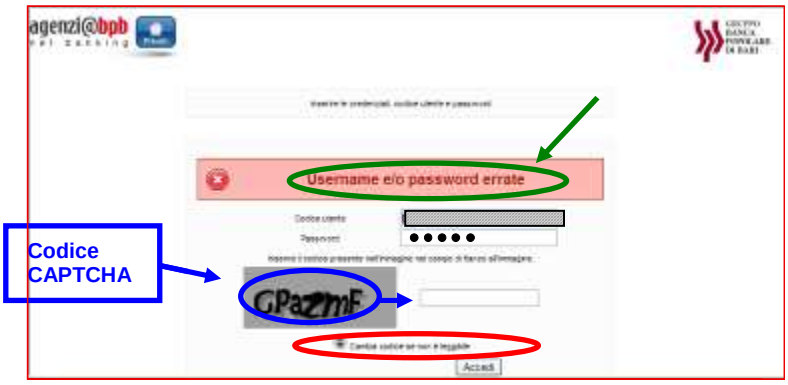
Diversamente, superato il numero di tentativi di errore consentiti, il sistema produce automaticamente, per motivi di sicurezza, il blocco dell'utenza (cfr. "ESEMPIO DI ERRORE CHE GENERA IL BLOCCO DELL'UTENZA" di seguito riportato).

In caso di blocco dell'utenza l'utente può richiedere lo sblocco della password direttamente on line, mediante la funzione di *AUTORESET*, senza recarsi in filiale.

Per l'utilizzo della funzione di "autoreset", è necessario seguire le istruzioni di seguito riportate (cfr. paragrafo ISTRUZIONI PER UTILIZZARE LA FUNZIONE "AUTORESET").

ESEMPIO DI ERRORE CHE NON GENERA IL BLOCCO DELL'UTENZA

Di seguito l'esempio più frequente di errore che non genera il blocco dell'utenza entro il numero di tentativi consentiti: errato inserimento della password e relativa digitazione del codice CAPTCHA per annullare l'errore e consentire l'indicazione del valore corretto.



Per rimediare all'errore di digitazione:

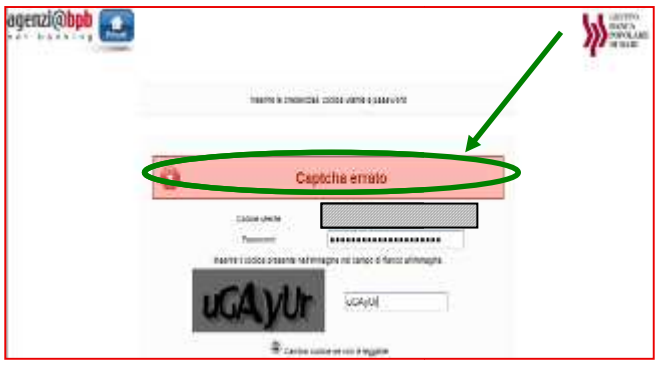
- Inserire nuovamente la password nel campo **Password** avendo cura di riportare il codice corretto.
- Digitare il codice visualizzato nell'immagine nel campo presente a fianco dell'immagine (denominato campo **CAPTCHA**).
  [Il CAPTCHA è una sequenza di lettere e numeri, generata automaticamente e in modo casuale, che appare distorta o offuscata sullo schermo].

- Nel caso in cui il codice risulti illeggibile all'utente, è possibile generarne un altro cliccando su "**Cambia codice se non è leggibile**" (cambio CAPTCHA).
- Premere il tasto **Accedi**.

N.B. Se l'errore di digitazione della password si ripete per più di cinque volte, l'utenza viene automaticamente bloccata dal sistema. In questo caso è necessario richiedere lo sblocco della password come riportato nel successivo paragrafo (cfr. paragrafo ISTRUZIONI PER UTILIZZARE LA FUNZIONE "AUTORESET").

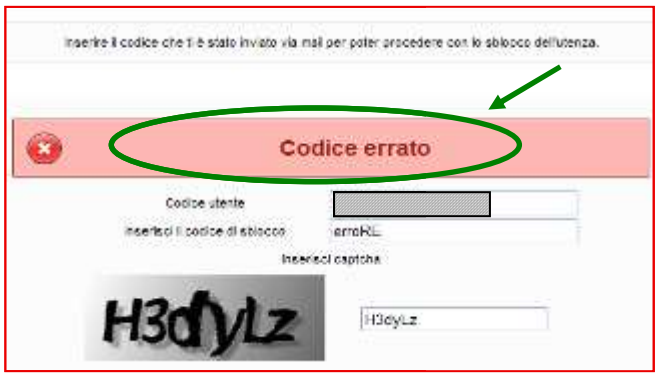
ESEMPI DI ERRORE CHE GENERANO IL <u>BLOCCO</u> DELL'UTENZA

Di seguito un esempio di errato inserimento del codice CAPTCHA per un numero di tentativi superiore a quello consentito, che provoca il **blocco dell'utenza**.



In questo caso è possibile richiedere lo sblocco della password utilizzando la <u>funzione di autoreset</u> (cfr. paragrafo ISTRUZIONI PER UTILIZZARE LA FUNZIONE "AUTORESET").

Di seguito un esempio di errato inserimento del codice di sblocco per più di cinque tentativi, che provoca il **blocco definitivo dell'utenza**.



In questo caso è necessario richiedere lo sblocco della password alla propria filiale.

ISTRUZIONI PER UTILIZZARE LA FUNZIONE "*AUTORESET*" (SBLOCCO *PASSWORD ONLINE*)

PREMESSA

La funzione di autoreset password di seguito presentata è attiva per i soli profili dispositivi (full o basic) in possesso di token (mobile o chiavetta fisica).
Per i profili informativi (in possesso di PIN) non è disponibile la funzionalità di autoreset, pertanto gli utenti con tale profilo dovranno rivolgersi alla propria filiale in caso di blocco dell'utenza.

Nell'accesso al servizio ***agenzi@bpb***, possono verificarsi errori di inserimento delle credenziali (codice utente, *password*, *token*) o di altri codici richiesti di volta in volta dalla procedura (codice *CAPTCHA*, ecc.) che comportano, al superamento del massimo numero di tentativi consentiti, il blocco dell'utenza.

Quando invece non viene superato il numero massimo di tentativi di errore possibili, il sistema di autenticazione richiede, in aggiunta alle credenziali, l'immissione di un codice *CAPTCHA* (ovvero un codice alfanumerico che deve essere copiato da un'immagine volutamente offuscata o distorta).

Il blocco dell'utenza non consente all'utente l'accesso al servizio anche nel caso in cui, a valle del blocco stesso, vengano inserite le credenziali corrette; in tale scenario l'utente dovrà accedere alla procedura di ***Autoreset online*** che consentirà lo sblocco dell'utenza mediante la creazione di una nuova *password* di accesso, e dunque l'automatico invalidamento della *password* precedente.

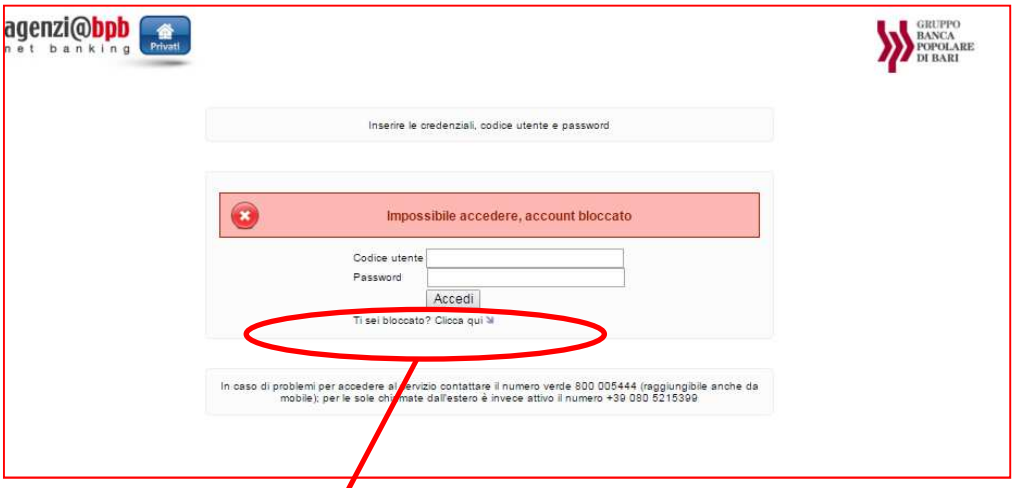
Per l'utilizzo della funzione di *Autoreset*, è necessario seguire le istruzioni di seguito riportate (cfr. paragrafo ISTRUZIONI PER UTILIZZARE LA FUNZIONE "AUTORESET").

Il servizio di Autoreset è disponibile esclusivamente sul sito www.agenziabpb.it.
In caso di blocco dell'utenza da *Mobile Banking*, per usufruire della funzione di *Autoreset* è necessario chiudere l'applicazione e collegarsi al sito *www.agenziabpb.it*.

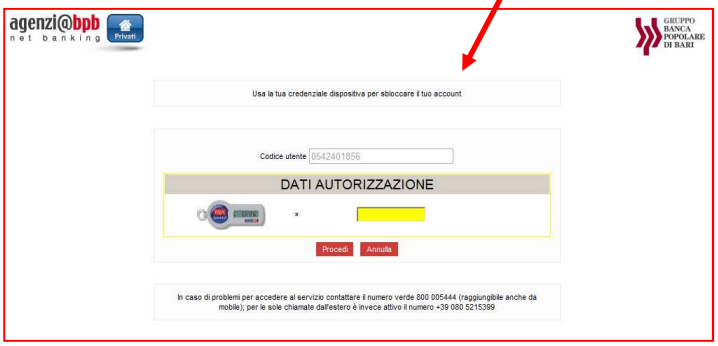
In altri casi particolari di errore che provocano un blocco definitivo dell'utenza, tra i quali lo stesso utilizzo non corretto della funzione di *Autoreset* (es. errato inserimento del codice di sblocco per più di tre tentativi), **è necessario richiedere lo sblocco della password alla propria filiale**.

ISTRUZIONI OPERATIVE PER LA FUNZIONE *AUTORESET*

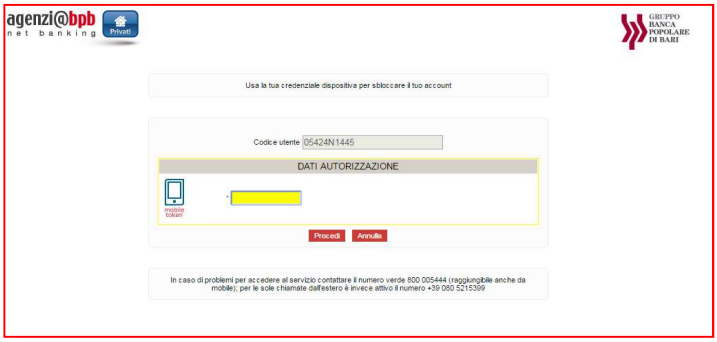
Il blocco dell'utenza viene comunicato all'utente con un messaggio di errore apposito che compare nella maschera di login a valle del verificarsi di determinati errori (es. dopo 5 errori di inserimento della password di accesso).
Di seguito si riportano le schermate della procedura di *autoreset password:*



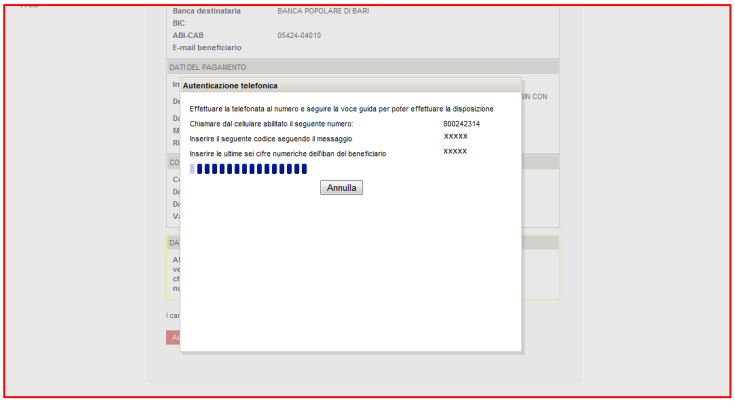
- Cliccare sulla freccia che si trova al termine della frase **Ti sei bloccato? Clicca qui ↘** , sotto il comando **Accedi**.



esempio Token chiavetta



esempio Mobile Token



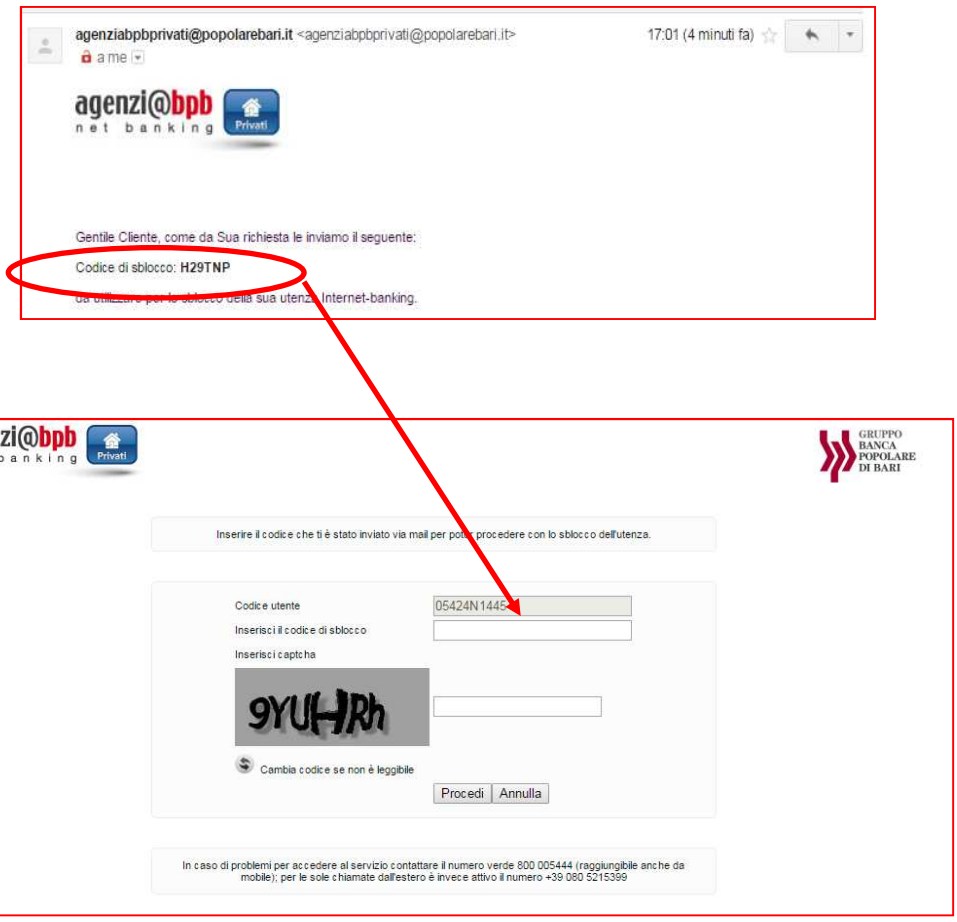
esempio secure call

- Inserire il codice OTP generato:
  - dalla chiavetta *token* (nel caso in cui l'utente abbia un *token* tradizionale)
  - dal *mobile token* (nel caso in cui l'utente abbia un *token* installato sul proprio *smartphone*).
  - nel caso di utilizzo del sistema secure call (clienti Tercas/Caripe) effettuare la chiamata al numero indicato e procedere con le istruzioni della voce guida
- Premere il tasto **Accedi**.
- A valle di questo procedimento il sistema genera automaticamente un **codice di sblocco** che viene recapitato via *mail* all'indirizzo di posta elettronica dell'utente (comunicato alla Banca al momento dell'attivazione del servizio di *internet banking agenzi@bpb* o successivamente modificato).

N.B. Ai fini dell'utilizzo della funzione di *Autoreset* è essenziale che l'indirizzo *mail* associato al servizio di *internet banking agenzi@bpb* sia valido ed attivo. Per verificare che l'indirizzo sia corretto, occorre accedere alla sezione **Servizi > Dati personali > Dati personali** del portale, ove è possibile consultare e modificare i dati personali comunicati alla Banca al momento dell'attivazione del servizio *agenzi@bpb* (indirizzo *mail* e numero di telefono cellulare).

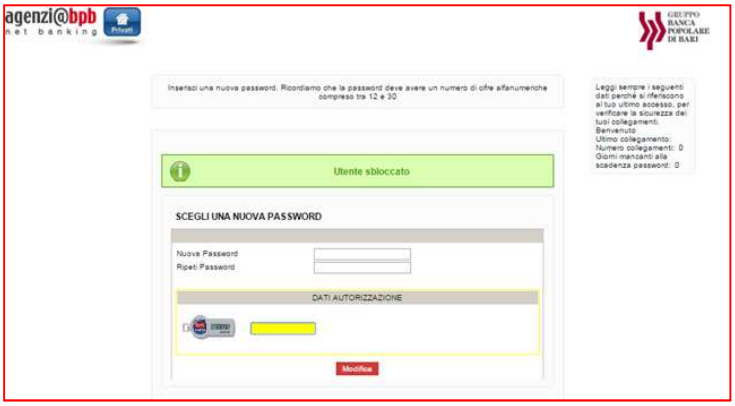
- Aprire l'email ricevuta (dal mittente agenziabpbprivati@popolarebari.it) sul proprio indirizzo di posta elettronica per recuperare il **Codice di sblocco** generato dal sistema.

Fac-simile mail di invio del codice di sblocco:

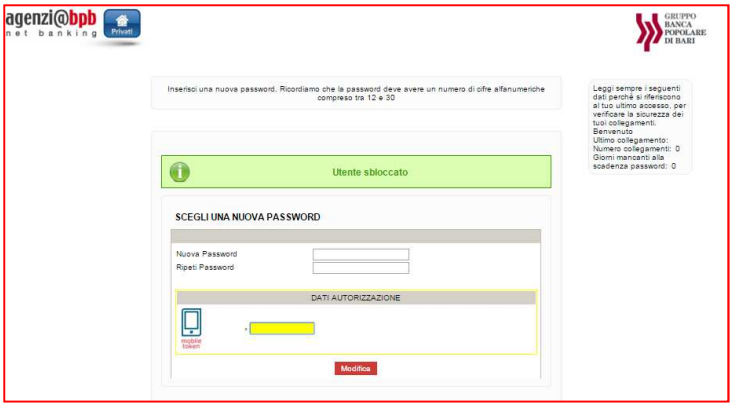


- Inserire nella procedura di autoreset il **Codice di sblocco** indicato nel messaggio di posta elettronica.
- Digitare il **Codice *CAPTCHA*** visualizzato nell'immagine. Nel caso in cui il codice risulti illeggibile all'utente, è possibile generarne un altro cliccando su "**Cambia codice se non è leggibile**" (cambio *CAPTCHA*).
- Premere il tasto **Procedi**.

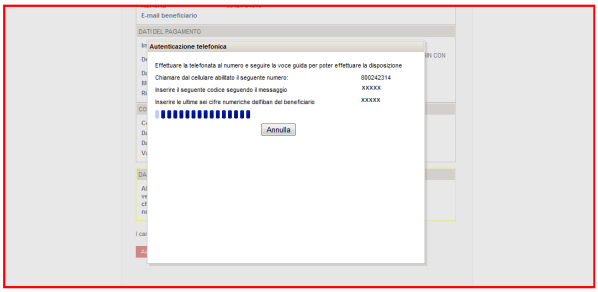
A questo punto la funzione di sblocco *password* è terminata correttamente: il sistema ha azzerato la *password* in uso e l'utente può creare in autonomia la **nuova *password*** di accesso.



esempio Token chiavetta



esempio Mobile Token



esempio secure call

- Creare una nuova password digitandola nel campo **Nuova Password** (numeri e lettere, minuscole e/o maiuscole **comprese tra 8 e 30 caratteri**).
- Confermare la nuova *password* creata digitandola nel campo **Ripeti Password.**
- Inserire il codice OTP generato:
  - dalla chiavetta *token* (nel caso in cui l'utente abbia un *token* tradizionale)
  - dal *mobile token* (nel caso in cui l'utente abbia un *token* installato sul proprio *smartphone*).
  - nel caso di utilizzo del sistema secure call (clienti Tercas/Caripe) effettuare la chiamata al numero indicato e procedere con le istruzioni della voce guida
- Premere il tasto **Modifica**.

L' utente può accedere nuovamente al servizio di internet banking utilizzando il proprio **Codice Utente** e la nuova **Password** appena creata.