

Strong Customer Authentication

Cos'è

Per aumentare il livello di sicurezza delle operazioni di pagamento, la normativa sui servizi di pagamento impone a tutti gli istituti finanziari di adottare strumenti che consentano ai clienti di **accedere alle proprie informazioni sui conti online e confermare i pagamenti elettronici** ovvero **disposti mediante canale a distanza** (es. online) in modo ancora più sicuro.

CheBanca! ha adottato la **Strong Customer Authentication**, un sistema di autenticazione forte del cliente basato sull'uso di due o più elementi classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce, come una password o un PIN), del possesso (qualcosa che solo l'utente possiede, come uno smartphone o un dispositivo personale) e dell'inerenza (qualcosa che caratterizza l'utente, come l'impronta digitale o altri dati biometrici).

CheBanca! mette a tua disposizione diverse **modalità** di Strong Customer Authentication.

Se disponi di uno smartphone Android o iOS, puoi attivare Smart App per autorizzare accessi e operazioni dall'App CheBanca! tramite un PIN personale.

Se non disponi di uno smartphone Android o iOS, puoi richiedere in Filiale o tramite Servizio Clienti il rilascio della matrice dispositiva e l'attivazione di Basic SMS. Con questa modalità di Strong Authentication, per autorizzare l'accesso alla tua area riservata e le principali operazioni disposte in autonomia ti verranno richiesti i codici della matrice dispositiva e la One-Time Password (c.d. OTP) di volta in volta ricevuta per SMS.

Se non disponi di un numero di cellulare italiano per ricevere gli SMS, puoi richiedere in Filiale o tramite Servizio Clienti il rilascio di un Token hardware con il quale generare di volta in volta l'OTP.

Smart App

COME ATTIVARLA

1. Scarica l'App CheBanca! da App Store o Google Play.
2. Accedi con i codici richiesti e seleziona la voce *Attiva Smart App*.
3. Verifica il numero di telefono in uso per l'attivazione di Smart App, confermando le ultime 4 cifre.
4. Inserisci il PIN temporaneo di 6 cifre ricevuto via SMS per completare l'attivazione.
5. Scegli e conferma il tuo PIN personale di 5 cifre.

Da questo momento, Smart App è attiva. Il PIN personale ti servirà per confermare le operazioni di pagamento che disponi dall'App CheBanca! e generare nell'App le OTP necessarie per operare da Area Clienti e tramite il Servizio Clienti.

COME AUTORIZZARE ACCESSI E OPERAZIONI

Per autorizzare il tuo accesso¹ e le principali operazioni **nell'App CheBanca!**, ti basta inserire dove richiesto il PIN personale di 5 cifre che hai scelto all'attivazione di Smart App.

Per autorizzare il tuo accesso e le principali operazioni **in Area Clienti**, ti viene richiesta l'autorizzazione dallo smartphone su cui è stata attivata Smart App. È quindi necessario avviare l'App CheBanca! e, prima di effettuare il login, selezionare la voce *Autorizza Operazioni*.

In questa sezione **per alcune operazioni** - quali, in particolare, bonifici SEPA, bonifici per agevolazioni fiscali, bonifici ricorrenti, bonifici SWIFT, ricariche telefoniche, pagamenti di bollette Telecom, MAV, RAV, RI.BA., bollettini postali bianchi e premarcati, bollettini Freccia e inserimento utenze - sarà visibile il **riepilogo dell'operazione in attesa di autorizzazione**. Per autorizzarla, una volta visualizzato il riepilogo sarà sufficiente inserire il PIN personale scelto in fase

¹ Resta ferma la necessità di inserire i tuoi codici personali; se previsto dal tuo dispositivo, potrai utilizzare il riconoscimento biometrico, invece di inserire tali codici ad ogni accesso. Per farlo, attiva l'opzione "Ricordami" disponibile al login nell'App CheBanca!.

CheBanca!

di attivazione di Smart App. Come previsto dalla normativa sui servizi di pagamento per tali transazioni online si applica il **Dynamic Linking**, un fattore di sicurezza che prevede requisiti aggiuntivi di autorizzazione, basati sul collegamento dinamico tra operazione, importo e beneficiario specificati dall'utente al momento di disporre il pagamento.

Per le operazioni sopra elencate, qualora il tuo dispositivo fosse offline ovvero non comunicasse correttamente con i sistemi della Banca e non fosse pertanto disponibile il riepilogo dell'operazione, per procedere con l'autorizzazione sarà sufficiente scansionare con il tuo dispositivo il **QR Code** visibile in Area Clienti (oppure digitare direttamente nell'App il corrispettivo codice identificativo), inserire nell'App il PIN personale, quindi digitare in Area Clienti il **codice di autorizzazione** così generato con l'App. Tale codice di autorizzazione – **Dynamic Linking** – consente di ricondurre direttamente l'azione dispositiva alla singola operazione, per un determinato importo e beneficiario, rappresentati nel riepilogo dell'operazione.

Per ulteriori informazioni in merito all'utilizzo di Smart App puoi consultare la Guida presente su chebanca.it > Sicurezza > Strong Authentication.

Per tutte le altre operazioni, all'interno della sezione *Autorizza Operazioni* dell'App CheBanca! è disponibile il generatore di OTP: è sufficiente inserire il **PIN personale** scelto all'attivazione di Smart App per generare l'**OTP** necessaria ad autorizzare l'operazione richiesta.

Ricorda:

- l'OTP e il codice di autorizzazione hanno una validità di 30 secondi. Una volta scaduta, puoi generarne una nuova con le stesse modalità;
- Smart App ti consente di generare le OTP e i codici di autorizzazione anche in assenza di connessione dati sul tuo dispositivo;
- è necessario verificare di inserire il PIN corretto: se inserisci il PIN personale in modo errato, le OTP e i codici di autorizzazione generati non saranno validi.

COSA FARE SE...

Hai perso il telefono?

Se hai perso o ti hanno rubato il telefono su cui hai installato l'App CheBanca!, nessuno potrà operare sui tuoi conti se non conosce il PIN personale che hai scelto per effettuare le operazioni. È tuttavia consigliabile **bloccare Smart App**.

Puoi farlo in 3 modi:

- selezionando la voce dedicata nell'accedere all'Area Clienti, dopo aver inserito codice cliente e codice di accesso;
- contattando il Servizio Clienti all'800.10.10.30 (dall'estero:+39.02.3200.4141);
- recandoti in qualsiasi Filiale CheBanca!.

Successivamente potrai eseguire il reset di Smart App e riattivarla nell'App CheBanca!.

Hai inserito troppe volte un PIN personale errato o l'hai dimenticato?

Per tutelare la sicurezza dei tuoi dati e dei tuoi prodotti, la funzionalità che consente di generare le OTP e i codici di autorizzazione viene bloccata quando il PIN personale risulta inserito per 5 volte consecutive in modo errato. Quando la funzionalità è bloccata non è possibile autorizzare accessi e operazioni.

In questo caso, puoi effettuare il **reset di Smart App** selezionando la voce dedicata che trovi nell'accedere alla tua Area Clienti, dopo aver inserito codice cliente e codice di accesso. Successivamente, potrai riattivarla dall'App CheBanca!.

Ricorda: se il tuo documento d'identità censito in CheBanca! è scaduto e la tua Smart App è bloccata, potrai richiederne il reset da Servizio Clienti oppure in Filiale.

Hai un telefono nuovo, su cui vuoi spostare Smart App?

È sufficiente attivare il servizio sul tuo nuovo dispositivo: le modalità di attivazione di Smart App non cambiano.

CheBanca!

Basic SMS

COME ATTIVARLA

Se non hai attiva alcuna modalità di Strong Customer Authentication, una volta in possesso della matrice dispositiva puoi attivare Basic SMS collegandoti a clienti.chebanca.it, inserendo codice cliente e codice di accesso e seguendo le indicazioni fornite.

Se hai attiva una modalità di Strong Customer Authentication, sei in possesso della matrice dispositiva e decidi di passare il Basic SMS, ecco come procedere:

1. accedi alla tua Area Clienti e vai al percorso *Il mio profilo > Strong Authentication*;
2. seleziona l'attivazione della modalità Basic SMS;
3. verifica e certifica il numero di telefono al quale desideri ricevere le OTP via SMS;
4. inserisci i codici della matrice dispositiva che corrispondono alle coordinate indicate;
5. inserisci il PIN temporaneo di 6 cifre ricevuto via SMS.

COME AUTORIZZARE ACCESSI E OPERAZIONI

Nell'App CheBanca! e in Area Clienti, per autorizzare il tuo accesso e le operazioni devi inserire i codici della matrice dispositiva che corrispondono alle coordinate indicate e, subito dopo, l'OTP ricevuta per SMS².

COSA FARE SE...

Hai perso il telefono?

Se hai perso o ti hanno rubato il telefono su cui ricevi gli SMS con le OTP, è consigliabile bloccare Basic Sms.

Le modalità a tua disposizione sono le stesse del blocco di Smart App:

- selezionando la voce dedicata nell'accedere all'Area Clienti, dopo aver inserito codice cliente e codice di accesso;
- contattando il Servizio Clienti all'800.10.10.30 (dall'estero:+39.02.3200.4141);
- recandoti in qualsiasi Filiale CheBanca!.

Hai inserito troppe volte un'OTP errata?

Per proteggerti da eventuali tentativi di frode, Basic SMS viene bloccata se l'OTP, utilizzata per confermare le operazioni dispositive, viene inserita per 5 volte in maniera errata. Quando la funzionalità è bloccata, non è possibile autorizzare accessi e operazioni..

In questo caso, puoi effettuare il **reset di Basic SMS** selezionando la voce dedicata che trovi nell'accedere alla tua Area Clienti, dopo aver inserito codice cliente e codice di accesso. Successivamente, potrai riattivarla allo stesso percorso.

Se preferisci, potrai passare a **Smart App** attivandola dall'App CheBanca!.

Hai un telefono nuovo?

Se hai un nuovo telefono ma il numero è lo stesso non cambia nulla: continuerai a ricevere gli SMS con le OTP.

Token

COME ATTIVARLO

Puoi attivare il Token hardware collegandoti a clienti.chebanca.it, inserendo codice cliente e codice di accesso e seguendo le indicazioni fornite.

² Come previsto dalla normativa sui servizi di pagamento ad alcune transazioni online – in particolare, bonifici SEPA, bonifici per agevolazioni fiscali, bonifici ricorrenti, bonifici SWIFT, ricariche telefoniche, pagamenti di bollette Telecom, MAV, RAV, RI.BA., bollettini postali bianchi e premarcati, bollettini Freccia e inserimento utenze – si applica il **Dynamic Linking**, un fattore di sicurezza che prevede requisiti aggiuntivi di autorizzazione, basati sul collegamento dinamico tra operazione, importo e beneficiario specificati dall'utente al momento di disporre il pagamento. Il codice che sarà trasmesso al cliente in tali casi sarà conforme a detti requisiti.

CheBanca!

COME AUTORIZZARE ACCESSI E OPERAZIONI

Per autorizzare l'accesso alla tua area riservata e le operazioni nell'App CheBanca! e in Area Clienti, ti viene richiesto di inserire un'OTP generata con il Token stesso.

Per autorizzare le operazioni in ambito Dynamic Linking³, è invece necessario scansionare il QR Code con il Token hardware (o digitare manualmente il codice identificativo dell'operazione) e inserire, in Area Clienti o in App, il codice di autorizzazione così generato.

COSA FARE SE...

Hai perso il Token?

Se hai perso o ti hanno rubato il Token hardware, puoi **bloccarlo** per impedire che venga utilizzato il generatore di OTP e codici di autorizzazione. Per farlo, seleziona la voce dedicata che trovi nell'accedere alla tua Area Clienti, dopo aver inserito codice cliente e codice di accesso. Successivamente, potrai sbloccarlo recandoti in Filiale o chiamando il Servizio Clienti all'800.10.10.30 (dall'estero: +39.02.3200.4141).

Casi di esenzione

In applicazione della normativa sui servizi di pagamento, CheBanca! ha previsto alcuni casi di esenzione dalla Strong Customer Authentication. In particolare con riferimento ai **bonifici ricorrenti**, l'autorizzazione mediante Strong Customer Authentication verrà richiesta solo al primo inserimento. I pagamenti successivi verranno effettuati automaticamente.

Inoltre, con riferimento alle **transazioni con carta di pagamento effettuate in modalità contactless** sono state previste delle soglie limite al di sotto delle quali non è richiesta alcuna forma di autenticazione forte. Più in dettaglio, non sarà necessaria l'autorizzazione mediante autenticazione forte per transazioni effettuate in modalità contactless di importo massimo pari a 25€ per ciascuna transazione. Nel momento in cui le transazioni cumulativamente superino la soglia di 150€, la presente esenzione non troverà applicazione e verrà richiesto al cliente l'utilizzo di una forma di autenticazione forte, anche con l'inserimento fisico della carta di pagamento nel terminale.

Tale soglia cumulativa è calcolata a partire dall'ultima transazione effettuata con l'inserimento fisico della carta oppure in modalità contactless, autorizzata con autenticazione forte.

Per assistenza o maggiori informazioni sulla Strong Customer Authentication, puoi contattare il Servizio Clienti all'800.10.10.30 (dall'estero: +39.02.3200.4141) oppure recarti in qualsiasi Filiale CheBanca!.

Consigli per la tua sicurezza

1. Custodisci con cura i tuoi **dati personali** e non comunicarli a terzi.
2. Modifica periodicamente il **codice di accesso** alla tua Area Clienti.
3. Scarica l'**App CheBanca!** solo dagli store ufficiali e, quando accedi alla tua **Area Clienti**, verifica che la connessione sia sicura.
4. Per avere sotto controllo i movimenti di carte e conti, attiva gli **alert** gratuiti via e-mail e App.
5. Presta attenzione alle email sospette: CheBanca! non ti chiederà mai di comunicare **informazioni riservate** (es. codici di accesso all'Area Clienti, dati delle carte) via email.

Se credi che qualcuno sia entrato in possesso dei tuoi codici di accesso o dispositivi, oppure se il telefono su cui è attiva Smart App o Basic SMS è stato rubato, ti invitiamo a bloccare la Strong Customer Authentication in autonomia dalla tua Area Clienti o contattare immediatamente il **Servizio Clienti** al numero **800.10.10.30** (dall'estero: +39.02.3200.4141).

³ Per saperne di più sul Dynamic Linking e su quali operazioni interessi, vedi la nota 2 del presente documento.