MEDIOBANCA PREMIER

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.

La Banca 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).

La Banca anche mediante i propri *Provider Partner,* 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 messa a disposizione dalla Banca che consentirà la generazione di un codice necessario per l'esecuzione delle operazioni richieste.

Se non disponi di uno smartphone Android o iOS, puoi richiedere il rilascio della matrice dispositiva e l'attivazione di Basic SMS tramite Servizio Clienti o in Filiale, qualora quest'ultima sia un canale disponibile. Con questa modalità di Strong Authentication, per autorizzare l'accesso alla tua area riservata e le principali operazioni disposte dai Canali Digitali 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, tramite Servizio Clienti o in Filiale, qualora quest'ultima sia un canale disponibile, il rilascio di un Token hardware con il quale generare di volta in volta l'OTP.

Ai fini dell'utilizzo della Carta di Debito, puoi accedere ed autorizzare le operazioni di pagamento secondo le modalità autorizzative messe a disposizione da Nexi Payments S.p.A., provider terzo di cui la Banca si avvale per la gestione delle carte di debito. A tal fine, conformemente alla normativa vigente, ti potrà essere richiesta una forma di autenticazione forte (ad esempio un codice dinamico e uno statico o biometria).

Smart App Mediobanca Premier

COME ATTIVARLA

1. Scarica l'App Mediobanca Premier da App Store, Google Play o Huawei AppGallery.
2. Accedi con i codici richiesti e seleziona *Attiva Smart App*.
3. Verifica il numero di cellulare sul quale vuoi attivare Smart App, confermandone le ultime 4 cifre.
4. Digita 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 Mediobanca Premier 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 accesso[1] e le principali operazioni **nell'App Mediobanca Premier,** è sufficiente 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 Mediobanca Premier e, prima di effettuare il login, selezionare la voce *Autorizza Operazioni*.

[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 Mediobanca Premier

Edizione 01/2024

In questa sezione **per alcune operazioni** - quali, in particolare, bonifici SEPA, bonifici per agevolazioni fiscali, bonifici ricorrenti, bonifici SWIFT, ricariche telefoniche, pagamenti di bollette, 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 di attivazione di Smart App. Il PIN Personale potrà essere inserito secondo le modalità tempo per tempo messe a disposizione dalla Banca.

Come previsto dalla normativa sui servizi di pagamento, per tali transazioni 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 mediobancapremier.com > Accesso e sicurezza > Strong Authentication.

Per tutte le altre operazioni, all'interno della sezione *Autorizza Operazioni* dell'App Mediobanca Premier 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.

Riconoscimento biometrico

A seguito della procedura di attivazione dell'App Mediobanca Premier se hai Smart App, puoi scegliere di **attivare anche la funzione di Strong Customer Authentication basata sul riconoscimento biometrico**. Potrai così accedere all'Area Clienti e all'App Mediobanca Premier e, se lo vorrai, decidere di eseguire anche le operazioni dispositive, utilizzando la tua impronta digitale o il riconoscimento facciale (o altre modalità biometriche messe a disposizione dal tuo device).

Per attivare il riconoscimento biometrico, che consente di accedere rapidamente all'Area Clienti e all'App Mediobanca Premier e autorizzare le operazioni, segui queste indicazioni:

1. accedi all'App Mediobanca Premier e, dal *Profilo*, seleziona *Sicurezza* e poi *Biometria*;
2. **scegli la funzionalità che desideri abilitare** tra "Accesso con biometria" e "Operatività con biometria":
   - selezionando "**Accesso con Biometria**" **accedi** all'Area Clienti e all'App Mediobanca Premier **utilizzando la biometria** (esempio l'impronta digitale o il riconoscimento facciale), **confermi le operazioni** continuando a utilizzare il PIN personale scelto durante l'attivazione di Smart App.

Per completare l'attivazione dell'"Accesso con Biometria" dovrai inserire il codice di 5 cifre che utilizzi per accedere alla tua area riservata (Codice di accesso);

- scegliendo "**Operatività con Biometria**" utilizzi la **funzionalità biometrica**, che richiama il PIN personale, anche per autorizzare le **operazioni dispositive**.

Per completare l'attivazione dell'"Operatività con Biometria" dovrai inserire il PIN personale scelto durante l'attivazione di Smart App.

Qualora non volessi più utilizzare il riconoscimento biometrico, potrai modificare le impostazioni in qualsiasi momento. In tal caso, per utilizzare nuovamente il riconoscimento biometrico, **dovrai riattivare la relativa funzionalità**.

Ricorda: attivando la biometria tutte le **impronte digitali** e/o il **riconoscimento facciale** e/o gli **altri elementi biometrici disponibili**, registrati nel tuo smartphone per l'identificazione del titolare, consentiranno di **accedere** ai conti e/o di **effettuare operazioni dispositive** attraverso il servizio Smart App di Mediobanca Premier. **Per la tua sicurezza**, ti ricordiamo che è fondamentale che tutte le **impronte digitali** e/o i **tratti somatici del volto** e/o **gli altri elementi biometrici disponibili,** registrati nel device che stai utilizzando ai fini identificativi, siano **esclusivamente tuoi**.

COSA FARE SE…

Hai perso lo smartphone?
Se hai perso o ti hanno rubato lo smartphone su cui hai installato l'App Mediobanca Premier, 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;
- recandoti in qualsiasi Filiale della Banca qualora sia un canale disponibile.

Successivamente potrai eseguire il reset di Smart App e riattivarla nell'App Mediobanca Premier.

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 Mediobanca Premier.

Ricorda: se il documento d'identità che ci hai fornito è nel frattempo scaduto e la tua Smart App è bloccata, potrai richiederne il reset tramite Servizio Clienti o in Filiale, qualora quest'ultima sia un canale disponibile.

Hai uno smartphone 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.

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.mediobancapremier.com, inserendo codice cliente e codice di accesso e seguendo le indicazioni fornite.

Se hai attiva una modalità di Strong Customer Authentication diversa da Basic SMS, sei in possesso della matrice dispositiva e decidi di passare a Basic SMS, puoi rivolgerti ai canali a tua disposizione (es. Servizio Clienti e/o Filiale qualora sia un canale previsto dai tuoi rapporti).

COME AUTORIZZARE ACCESSI E OPERAZIONI

In Area Clienti e in App Mediobanca Premier, 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 SMS[2].

[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, 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.

COSA FARE SE…

Hai perso lo smartphone?
Se hai perso o ti hanno rubato lo smartphone 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;
- recandoti in qualsiasi Filiale della Banca qualora sia un canale disponibile.

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 Mediobanca Premier.

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

Token Hardware

COME ATTIVARLO

Puoi attivare il Token Hardware collegandoti a clienti.mediobancapremier.com, inserendo codice cliente e codice di accesso e seguendo le indicazioni fornite.

COME AUTORIZZARE ACCESSI E OPERAZIONI
Per autorizzare l'accesso alla tua area riservata e le operazioni nell'App Mediobanca Premier e in Area Clienti, ti viene richiesto di inserire un'OTP generata con il Token stesso.
Per autorizzare le operazioni in ambito Dynamic Linking[3], 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 i 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 chiedere l'emissione di un nuovo Token Hardware tramite Servizio Cliente o in Filiale, qualora quest'ultima sia un canale disponibile.

Hai inserito troppe volte un PIN errato?
Per generare le OTP e i codici di autorizzazione, è necessario avviare il Token Hardware inserendo il PIN personale scelto all'attivazione del Token stesso. Per proteggerti da eventuali tentativi di frode, il Token Hardware viene bloccato quando il PIN risulta inserito per 5 volte consecutive in modo errato. Quando il Token è bloccato, non è possibile effettuare accessi e operazioni. In questo caso, tramite Servizio Clienti o in Filiale, qualora quest'ultima sia un canale disponibile, puoi chiederne lo sblocco o l'attivazione di una diversa modalità di Strong Authentication.

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

MEDIOBANCA PREMIER

Strong Customer Authentication - Carte di Debito e Carta di Credito Mediobanca Premier gestita in partnership con Nexi

Ai fini dell'utilizzo delle Carte di Debito e della Carta di Credito Mediobanca Premier gestita in partnership con Nexi, puoi accedere alla tua posizione (tramite portale dedicato accessibile da Area Clienti e APP Mediobanca Premier, App Nexi Pay e Area Personale su nexi.it) ed autorizzare le operazioni di pagamento secondo le modalità di autenticazione messe a tua disposizione in conformità alla normativa vigente da Nexi Payments S.p.A., provider terzo di cui la Banca si avvale per la gestione delle carte di pagamento.

Il servizio è valido solo per i possessori delle Carte di Debito e di Carta di Credito Mediobanca Premier gestita in partnership con Nexi (di seguito "Carte di Pagamento").

Per poter effettuare i pagamenti online sarà richiesto l'inserimento del codice di sicurezza Key6 scelto dal cliente e di un codice OTP che il cliente riceve al momento dell'operazione.

Nexi Payments S.p.A. consente, inoltre, l'accesso, l'effettuazione di operazioni dispositive e di pagamenti online tramite identificazione biometrica.

COME ATTIVARLI

Ai fini dell'utilizzo del codice di sicurezza Key6 unitamente all'OTP è necessario seguire i seguenti step:

1) accedere al portale dedicato da Area Clienti e App Mediobanca Premier, all'App Nexi Pay o all'Area Personale su nexi.it
2) scegliere il codice di sicurezza Nexi Key6 che ti verrà richiesto al primo accesso
3) selezionare *Profilo*, *Modalità di Accesso* e impostare *Accesso con password* (questo passaggio è necessario solo in caso di accesso da App Nexi Pay)
4) confermare l'identità inserendo il codice a 6 cifre ricevuto tramite SMS

Ai fini dell'utilizzo della Biometria è necessario seguire i seguenti step:

1) accedere all' App Nexi Pay
2) selezionare *Profilo*, *Modalità di Accesso* e impostare *Accesso tramite Biometria*
3) inserire l'impronta o inquadrare il viso per il riconoscimento facciale (a seconda della modalità prescelta/disponibile)
4) confermare l'identità inserendo il codice a 6 cifre ricevuto tramite SMS
5) attivare le notifiche dal proprio device iOS/Android

COME AUTORIZZARE OPERAZIONI

Per confermare un'operazione inerente alle Carte di Pagamento (es. PIN View) sarà necessario l'utilizzo dell'identificazione biometrica con il metodo scelto o, in alternativa, il codice OTP ricevuto via SMS.

Per confermare un'operazione online che richiede la SCA, ad esempio un'operazione di pagamento, ove previsto dal sistema e nel rispetto della normativa vigente, è necessario utilizzare una delle seguenti modalità di autenticazione forte messe a disposizione da Nexi:

a) se sei registrato all'App Nexi Pay, a fronte della ricezione della notifica autorizzativa sul tuo Smartphone, tramite impronta digitale o riconoscimento facciale su device abilitati al riconoscimento biometrico

b) se non sei registrato all'App Nexi Pay – o se l'App Nexi Pay non supporta, anche momentaneamente, il riconoscimento biometrico – inserendo sul sito dell'Esercente:

- il codice sicurezza Nexi Key6, ossia il codice numerico associato ad ogni carta del Titolare, che il Titolare stesso definisce come sopra indicato
- il codice di sicurezza OTP (One Time Password), ricevuto tramite SMS sul proprio cellulare.

COSA FARE SE…

Hai perso lo smartphone?

Se hai perso o ti hanno rubato lo smartphone su cui hai Nexi Pay, nessuno potrà effettuare operazioni di pagamento se non conosce il codice Key6: inoltre, essendo la biometria un fattore univoco non è possibile utilizzare l'App. In qualsiasi caso potrai contattare immediatamente il Servizio Clienti Nexi (attivo 24 ore su 24) per:

- bloccare immediatamente la tua Carta, e richiedere la cancellazione dell'utenza di accesso all'App Nexi Pay o all'Area Personale su nexi.it;
- verificare e, nel caso, contestare eventuali pagamenti sospetti.

Edizione 01/2024

MEDIOBANCA PREMIER

Hai uno smartphone che non supporta la biometria?

Se il tuo smartphone non è compatibile con la biometria potrai comunque autorizzare le operazioni tramite codice Nexi Key6 e OTP ricevuta via SMS.

Casi di esenzione

In applicazione della normativa sui servizi di pagamento, la Banca 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** (che consiste nel solo avvicinamento della carta all'apposito lettore senza l'introduzione di ulteriori forme di autorizzazione), 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 pari o inferiore a 50€ su circuito Debit Mastercard o Mastercard 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.

Infine, con riferimento alle transazioni a distanza con le Carte di Pagamento, non sarà richiesta l'applicazione della Strong Customer Authentication qualora siano soddisfatte tutte le seguenti condizioni:

a) l'importo dell'operazione di pagamento elettronico a distanza non supera i 30 Euro; e

b) l'importo cumulativo delle precedenti operazioni di pagamento elettronico a distanza, a prescindere dall'esercente, disposte dal cliente dall'ultima applicazione della Strong Customer Authentication non supera i 100 Euro.

In caso di raggiungimento anche di una sola delle soglie indicate, la Banca richiederà l'applicazione della Strong Customer Authentication. Resta ferma la facoltà della Banca di richiedere comunque l'applicazione della Strong Customer Authentication per ragioni di sicurezza, quando ritenuto necessario.

Per assistenza o maggiori informazioni sulla Strong Customer Authentication, puoi contattare il Servizio Clienti +39 02.32004141 da cellulare e dall'estero, 800.10.10.30 da rete fissa in Italia oppure, qualora sia un canale disponibile, puoi recarti in qualsiasi Filiale Mediobanca Premier.

Consigli per la tua sicurezza

1. Custodisci con cura i **Codici identificativi** e non comunicarli a terzi.
2. Modifica periodicamente il **Codice di accesso**: puoi farlo in autonomia da Area Clienti.
3. Scarica l'**App** Mediobanca Premier solo dagli store ufficiali e quando accedi alla tua **Area Clienti** verifica che la connessione sia sicura.
4. Attiva gli **alert** gratuiti che ti permettono di avere sotto controllo i movimenti di carte e conti: li ricevi via e-mail e/o tramite notifica push.
5. Presta attenzione alle e-mail sospette. Non ti chiederemo mai di comunicare **informazioni riservate**, come ad esempio i codici identificativi o i dati delle Carte.

Se qualcuno è entrato in possesso dei tuoi codici di accesso o dispositivi, oppure se ti è stato rubato lo smartphone, blocca tempestivamente la Strong Authentication. Puoi farlo in autonomia, contattando il Servizio Clienti oppure recandoti in Filiale, qualora sia un canale disponibile.

Il Servizio Clienti è a disposizione ai seguenti numeri:

- 800.10.10.30 da rete fissa in Italia;
- +39 02.3200.4141 da cellulare o dall'estero.

Edizione 01/2024