



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.

Mediobanca Premier 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).

Mediobanca Premier, anche mediante i propri *Provider Partner*, mette a disposizione del Cliente diverse **modalità** di Strong Customer Authentication.

Per accedere e autorizzare operazioni dall'area personale del sito mediobancapremier.com ("**Area Clienti**"), è possibile utilizzare la modalità di autenticazione tramite credenziali, come di seguito illustrato. Con questa modalità di Strong Authentication, potranno essere richiesti i codici identificativi e/o la One-Time Password (c.d. OTP) di volta in volta ricevuta per SMS.

Si ricorda che per l'utilizzo della Strong Authentication e, quindi, per l'accesso all'area personale e per disporre le operazioni tramite canale a distanza è necessario essere in possesso di un numero di cellulare italiano.

Ai fini dell'utilizzo della Carta di Debito Business International (ove rilasciata), è possibile accedere ed autorizzare le operazioni di pagamento secondo le modalità autorizzative messe a disposizione da Nexi Payments S.p.A., Provider Partner di cui la Banca si avvale per la gestione delle carte di debito. A tal fine, conformemente alla normativa vigente, potrà essere richiesta al cliente una forma di autenticazione forte (ad esempio un codice dinamico e uno statico o biometria). Le modalità di autenticazione forte applicabili sono descritte al successivo paragrafo "Strong Customer Authentication - Carta di Debito Business International".

Strong Customer Authentication – Servizi di Internet Banking di Mediobanca Premier

CODICI DI IDENTIFICAZIONE E OTP VIA SMS

COME ATTIVARLA

Al primo accesso all'area personale del sito mediobancapremier.com ("**Area Clienti**"), verrà richiesto di effettuare le seguenti operazioni:

1. inserimento dei codici di identificazione (Codice Cliente e Codice di accesso provvisorio) fornite da Mediobanca Premier;
2. verifica dell'indirizzo email fornito alla Banca seguendo le indicazioni contenute nell'email di verifica;
3. verifica del numero di cellulare fornito alla Banca inserendo il codice temporaneo di 6 cifre ricevuto via SMS;
4. modifica del Codice di accesso provvisorio fornito dalla Banca, scegliendo un Codice di accesso personale di 5 cifre (PIN).

COME AUTORIZZARE ACCESSI E OPERAZIONI

Per **accedere** all'Area Clienti sarà richiesto di inserire il Codice Cliente, il Codice di accesso di 5 cifre che è stato scelto e il codice OTP di 6 cifre ricevuto via SMS al numero di telefono associato.

Per **autorizzare** le principali operazioni in Area Clienti basterà inserire il codice OTP di 6 cifre ricevuto tramite SMS al numero di telefono associato. Prima di autorizzare qualsiasi operazione è possibile visualizzare il riepilogo dell'operazione e verificarne la correttezza di tutti i dati inseriti.

Ricordiamo che:

- l'OTP ha validità di 300 secondi (5 minuti). Una volta scaduto si potrà richiedere l'invio di un nuovo codice.
- È necessario verificare di inserire l'OTP corretto: se vengono inseriti OTP errati l'operazione non verrà eseguita.



COSA FARE SE...

Hai perso lo smartphone o il device abilitato?

Se hai perso o ti hanno rubato lo smartphone su cui ricevi gli SMS con le OTP, è consigliabile bloccare i codici identificativi con le modalità tempo per tempo messe a disposizione dalla Banca.

Hai inserito troppe volte un'OTP errata?

Per proteggerti da eventuali tentativi di frode, i codici di identificazione verranno bloccati se l'OTP, utilizzata per confermare le operazioni dispositive, viene inserita per 5 volte in maniera errata. Quando i codici sono bloccati, non è possibile autorizzare accessi e operazioni.

A seguito del blocco dei codici di identificazione è necessario contattare la Banca per chiedere una nuova emissione di credenziali.

Vuoi bloccare o sospendere le tue credenziali di accesso?

In Area Clienti è possibile bloccare le tue credenziali di accesso accedendo alla sezione Privacy e Sicurezza. Oltre ad indicare il motivo della richiesta di blocco, sarà possibile richiedere contestualmente anche la riemissione di nuove credenziali.

Ove la richiesta di nuove credenziali venga fatta successivamente alla richiesta di blocco, il Cliente potrà rivolgersi ai canali tempo per tempo messi a sua disposizione da parte della Banca.

In Area Clienti sarà inoltre possibile richiedere la sospensione temporanea delle credenziali di accesso. Lo sblocco delle credenziali potrà essere richiesto rivolgendosi ai canali tempo per tempo messi a sua disposizione da parte della Banca.

Attualmente il Cliente potrà rivolgersi al **Servizio Clienti** al numero **+39 02.32004141 da cellulare e dall'estero o al numero 800.10.10.30 da rete fissa in Italia**, al proprio Advisor di riferimento oppure recarsi in qualsiasi Filiale Mediobanca Premier.

Hai un nuovo smartphone?

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

Strong Customer Authentication - Carta di Debito Business International

Ai fini dell'utilizzo della Carta di Debito Business International, è possibile accedere alla posizione ed autorizzare le operazioni di pagamento secondo le modalità di autenticazione messe a disposizione in conformità alla normativa vigente da Nexi Payments S.p.A., provider terzo di cui la Banca si avvale per la gestione della Carta di Debito Business International.

Il servizio è valido solo per i possessori di Carta di Debito Business International.

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 accessibile 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 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 la modalità di accesso tramite Biometria
- 3) Inserire 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 alla Carta di Debito Business International (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.

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, Mediobanca Premier 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 Euro su circuito Debit Mastercard o Mastercard per ciascuna transazione. Nel momento in cui le transazioni cumulativamente superino la soglia di 150 Euro, 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 Carta di Debito Business International, 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, Mediobanca Premier 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 ulteriori informazioni sulla Strong Customer Authentication, puoi rivolgerti al tuo Advisor di riferimento oppure recarti in qualsiasi Filiale Mediobanca Premier.

In alternativa puoi contattare:

- per l'autenticazione relativa ai Servizi di Internet Banking Business, il Servizio Clienti di Mediobanca Premier al numero +39 02.32004141 da cellulare e dall'estero e al numero 800.10.10.30 da rete fissa in Italia;
- per l'autenticazione relativa alla Carta di Debito Business, il numero 02.345.444* (dall'estero: +39 02.34980.020**; dagli USA: 1.800.473.6896***).

* numero soggetto a tariffazione urbana secondo l'operatore telefonico utilizzato.

** è possibile effettuare chiamate a carico di Nexi.

*** numero verde accessibile soltanto da una linea telefonica USA, fissa o mobile.

Consigli per la tua sicurezza

1. Custodisci con cura le **credenziali** ed i **codici di accesso** e non comunicarli a terzi.
2. Modifica periodicamente il **codice di accesso** dalla tua Area Clienti.
3. 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.

Presta attenzione alle e-mail sospette. Non ti chiederemo mai di comunicare informazioni riservate, come ad esempio credenziali e codici di accesso o i dati delle Carte. Se credi che qualcuno sia entrato in possesso dei tuoi codici di accesso o dispositivi, oppure se il device associato che utilizzi per autorizzare accessi e operazioni 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 **+39 02.32004141 da cellulare e dall'estero o al numero 800.10.10.30 da rete fissa in Italia**.