Digital Banking

INFORMAZIONI SULLA BANCA

Banca Monte dei Paschi di Siena S.p.A.
Sede sociale in Siena, Piazza Salimbeni, 3
Numero verde 800.41.41.41
e-mail info@mps.it / sito internet www.mps.it
Cod. Fisc. e n. iscrizione al Registro delle Imprese di Siena: 00884060526 - Gruppo IVA MPS - Partita IVA 01483500524 Gruppo Bancario Monte dei Paschi di Siena - Codice Banca 1030.6 - Codice Gruppo 1030.6
Iscritta all'Albo presso la Banca d'Italia al n. 5274
Aderente al Fondo Interbancario di Tutela dei Depositi ed al Fondo Nazionale di Garanzia

(Qualora il prodotto sia offerto fuori sede)
Nome e Cognome del soggetto che entra in contatto con il Cliente
Indirizzo
Telefono e-mail
Qualifica (per i soggetti iscritti in albi o elenchi, indicare anche gli estremi)
Nome e cognome del Cliente cui il modulo è stato consegnato

Data Firma per avvenuta ricezione

CHE COS'E' IL DIGITAL BANKING

Digital Banking consente al Cliente di effettuare le operazioni di interrogazione e di disposizione sui Rapporti (es.: Conto Corrente, Deposito Titoli) tramite ogni canale diretto disponibile: Internet Banking, Banca Telefonica e ATM Cardless.
Digital Banking fornisce a ogni Cliente una Identità Digitale, costituita da:
- Codice Utente e Password che garantiscono la stessa modalità di autenticazione sui diversi canali;
- Contatti convalidati (Email e numero di cellulare);
- Firma Digitale Remota (valida per la sottoscrizione di contratti con Banca Monte dei Paschi di Siena);
- Posta Elettronica Certificata (nome.cognome@mpspec.it).

Per maggiori dettagli sui servizi di Firma Digitale Remota e Posta Elettronica Certificata forniti dalla Banca, si rimanda all'apposita sezione del presente documento.

Destinatari
Digital Banking è rivolto a tutta la Clientela privata (Singole Persone Fisiche) e consente di operare tramite i canali Internet Banking, Banca Telefonica e ATM Cardless.

Sistema di Autenticazione
All'atto della sottoscrizione di Digital Banking, il Cliente comunica alla Banca:
- Il Codice Utente di 8 cifre;
- Il numero di cellulare personale sul quale ricevere la Password Monouso, detta Codice di Conferma, e le notifiche;
- L'Email personale sulla quale ricevere le notifiche e che, se il Cliente lo desidera, può essere utilizzata come alternativa al Codice Utente, per accedere ai Canali tecnicamente abilitati.

La Banca consegna ai Clienti che hanno sottoscritto Digital Banking:
- La Password di 8 cifre, che il Cliente deve cambiare al primo utilizzo.

Digital Banking richiede al Cliente di inserire una Password Monouso, detta Codice di Conferma, sia per l'accesso sia per confermare ogni disposizione eseguita. Il Codice di Conferma viene inviato esclusivamente via SMS al numero cellulare indicato dal Cliente.

Operazioni
Con Digital Banking si possono effettuare operazioni sia di tipo informativo che dispositivo. Riportiamo di seguito le principali funzionalità:
- Lista saldo e movimenti del conto;
- Bonifici e pagamenti bollettini;

- Ricarica cellulari;
- Ricarica carte prepagate;
- Negoziazione titoli e quotazioni di borsa in tempo reale;
- Ricezione e consultazione estratto conto e altri documenti.

La lista completa delle funzionalità offerte da Digital Banking è disponibile sul sito della Banca www.mps.it nelle pagine dedicate al servizio.

Rischi tipici

Per l'informativa relativi ai rischi connessi all'uso di Digital Banking, si rimanda alla sezione dedicata nel presente documento.

PRINCIPALI CONDIZIONI ECONOMICHE

N.B.: *le condizioni economiche sotto riportate sono indicate nella misura minima (se a favore del Cliente) e massima (se a carico del Cliente), sono valide fino a nuovo avviso e non tengono conto di eventuali particolari spese aggiuntive, sostenute e/o reclamate da terzi o previste da specifici accordi in deroga, imposte o quant'altro dovuto per legge, che non sia immediatamente quantificabile; tali eventuali oneri aggiuntivi saranno oggetto di recupero integrale a parte.*

Le voci di spesa di seguito indicate si riferiscono a Digital Banking. Tramite i canali telematici è altresì possibile eseguire operazioni (es. bonifici, ricariche, compravendite titoli) sui Rapporti (es.: conti correnti, carte di pagamento e depositi titoli); per le condizioni economiche relative a tali operazioni è possibile consultare i fogli informativi dei prodotti/servizi di riferimento.

Condizioni economiche del servizio	

Digital Banking	
Canone Internet Banking e ATM Cardless	Esente
Canone Banca Telefonica	Esente

Servizio messaggi	
Notifiche SMS	€ 0,20
Notifiche SMS DocumentiOnLine	€ 0,20
Trading alert SMS	€ 0,30

SMS password monouso	
Per ogni SMS	€ 0,00

SMS per richieste di informazioni	
Per ogni SMS ricevuto	€ 0,20
Per ogni SMS inviato (secondo le tariffe previste dal gestore)	A carico del Cliente

Costi telefonici di collegamento	
Chiamate al numero verde del servizio Banca Telefonica	€ 0,00
Chiamate dall'estero al servizio Banca Telefonica	A carico del Cliente

ATM cardless	
Commissione prelievo diretto da CC su ATM/Cassa Automatica	€ 0,00
Valuta di addebito prelievo diretto da CC su ATM/cassa automatica	Giorno dell'operazione
Limite giornaliero prelievo diretto da CC su ATM	€ 1.550,00
Limite mensile prelievo diretto da CC su ATM	€ 1.550,00
Numero massimo giornaliero operazioni prelievo diretto da CC su ATM	3
Limite giornaliero prelievo diretto da CC su cassa automatica	€ 4.999,99
Limite mensile prelievo diretto da CC su cassa automatica	Nessun limite
Numero massimo giornaliero operazioni prelievo diretto da CC su cassa automatica	5
Commissione cambio taglio banconote su cassa automatica	€ 0,50
Limite giornaliero cambio taglio banconote su cassa automatica	€ 500,00

Quotazioni	
Canone quotazioni su mercati italiani in tempo differito	€ 0,00
Canone quotazioni su mercati italiani in tempo reale	€ 1,50
Canone quotazioni su mercati europei in tempo differito	€ 0,00
Canone quotazioni su mercati europei in tempo reale	€ 42,00
Canone quotazioni su mercati americani in tempo differito	€ 0,00
Canone quotazioni su mercati americani in tempo reale	€ 5,00
Periodicita' addebito canone quotazioni	Mensile

Massimali	
Limite giornaliero per operazioni di pagamento	€ 2.500,00
Limite giornaliero per operazioni di trasferimento fondi	€ 15.000,00
Limite giornaliero per operazioni di compravendita titoli	€ 500.000,00

Spese di spedizione delle comunicazioni. Le spese di spedizione sono riportate nel documento "Tariffe applicate alla clientela per la spedizione di comunicazioni e carnet assegni", pubblicato all'interno della sezione "Trasparenza - Servizi diversi" del sito internet della Banca (www.mps.it/trasparenza) e disponibile in filiale. Tali spese potranno subire variazioni in relazione al costo effettivamente sostenuto dalla Banca, in conformità a quanto previsto dall'art.127-bis TUB, e non sono applicate in caso di invio delle comunicazioni per canale elettronico.

SERVIZI DI FIRMA DIGITALE REMOTA E POSTA ELETTRONICA CERTIFICATA

L'attivazione del servizio di Firma Digitale Remota (FDR) e del servizio di Posta Elettronica Certificata (PEC) è facoltativa.
Attraverso l'utilizzo della FDR, il Cliente può sottoscrivere contratti e, più in generale, assumere impegni e rilasciare dichiarazioni esclusivamente nell'ambito dei rapporti intrattenuti con la Banca. La PEC, invece, può essere utilizzata dal Cliente per comunicare anche con soggetti terzi diversi dalla Banca.
Il Servizio FDR e il Servizio PEC hanno, rispettivamente, durata triennale dall'emissione del certificato di firma e durata annuale dalla attivazione della casella e sono erogati da InfoCert S.p.A. senza spese per il Cliente sino alle predette scadenze.
Il rinnovo del servizio PEC sarà effettuato alle condizioni comunicate per tempo da InfoCert S.p.A., restando inteso che è fatto salvo il diritto di recesso per il Cliente, esercitabile per entrambi i servizi in qualunque momento secondo le modalità descritte su www.mps.it.

RECESSO

Recesso dal contratto
Il Cliente può recedere dal contratto in qualsiasi momento, senza penalità e senza spese di chiusura del rapporto, con preavviso di almeno 30 giorni rispetto alla data di efficacia del recesso.

La Banca può recedere dal contratto con comunicazione consegnata al Cliente o inviata tramite Posta Elettronica Certificata o modalità equivalente con un preavviso minimo di due mesi.

Il Cliente e la Banca, in presenza di giusta causa o giustificato motivo, possono recedere dal contratto senza preavviso alcuno.

RECLAMI E SISTEMI DI RISOLUZIONE STRAGIUDIZIALE DELLE CONTROVERSIE

Il Cliente può presentare un Reclamo alla Banca:
- per posta ordinaria a Ufficio Reclami Banca Monte dei Paschi di Siena S.p.A. , viale Pietro Toselli, 60 - Cap. 53100 – Siena;
- per posta elettronica al seguente indirizzo: reclami@mps.it;
- per posta elettronica certificata (PEC) al seguente indirizzo: customercare@postacert.gruppo.mps.it;
- allo sportello dove è intrattenuto il rapporto o presso altri punti operativi della Banca;
- online compilando l'apposito form presente nella sezione "Reclami e Ricorsi" sul sito www.mps.it;

La Banca deve rispondere entro 60 giorni dal ricevimento.

Per i servizi di pagamento, la Banca deve rispondere entro 15 giorni dal ricevimento. In situazioni eccezionali, se la Banca non può rispondere entro 15 giornate operative per motivi indipendenti dalla sua volontà, è tenuta a inviare una risposta interlocutoria, indicando chiaramente le ragioni del ritardo nella risposta al reclamo e specificando il termine entro il quale l'utente di servizi di

pagamento otterrà una risposta definitiva. In ogni caso il termine per la ricezione della risposta definitiva non supera le 35 giornate operative. Fanno eccezione i reclami relativi a possibile violazione delle norme afferenti al "Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti" per cui i tempi massimi di riscontro sono 30 giorni lavorativi (prorogabili per ulteriori due mesi in casi eccezionali e motivati) così come previsto dall'art. 12 comma 3 del Regolamento Europeo 2016/679 (GDPR).
Qualora il Cliente non si ritenga soddisfatto della risposta, o non abbia ricevuto riscontro al reclamo nei termini previsti, può sottoporre la controversia all'Arbitro Bancario Finanziario (ABF), organismo di risoluzione delle controversie istituito presso la Banca d'Italia ai sensi dell'art. 128 bis del D.Lgs. 385/93 (Testo Unico Bancario), secondo le modalità indicate nella "Guida Pratica ABF", reperibile sul sito web www.arbitrobancariofinanziario.it, presso i locali della Banca oppure sul sito www.mps.it (attivabile solo dal Cliente e per le sole controversie relative ai servizi bancari).

Le modalità di invio dei ricorsi sono reperibili sulla guida disponibile presso le filiali della Banca e sul sito www.mps.it.

Il Cliente, in alternativa al ricorso all'ABF, può attivare una procedura di mediazione ai sensi dell'art. 5, comma 1 bis, del D.Lgs. 28/2010. La procedura di mediazione può essere esperita, singolarmente dal Cliente o in forma congiunta con la Banca, innanzi al Conciliatore Bancario Finanziario - Associazione per la soluzione delle controversie Bancarie, finanziarie e societarie - ADR (www.conciliatorebancario.it).

Se il Cliente intende rivolgersi all'Autorità Giudiziaria per una controversia relativa all'interpretazione ed applicazione di un contratto, concluso con la Banca, avente ad oggetto la prestazione di servizi bancari e/o finanziari dovrà esperire preventivamente - pena l'improcedibilità della relativa domanda - una delle procedure di risoluzione delle controversie o di mediazione summenzionate.

Inoltre, previo accordo delle Parti, è possibile rivolgersi anche ad organismi di mediazione diversi da quelli sopra, purché iscritti nell'apposito Registro presso il Ministero di Giustizia e precipuamente specializzati in materia bancaria/finanziaria.

RISCHI TIPICI

Alla luce del rischio di sicurezza delle operazioni eseguite mediante Digital Banking (es. a causa di hacker, illecita appropriazione di chiavi di sicurezza e/o dati, ecc.) e poiché il Cliente verrà identificato dalla Banca esclusivamente mediante la verifica del Sistema di Autenticazione, lo stesso è tenuto a mantenere segreti e riservati tutti i codici, i dispositivi e le procedure utilizzate per accedere e utilizzare Digital Banking.

Per tale ragione il Cliente si impegna a conservare correttamente il Sistema di Autenticazione e a custodirlo con la massima cura e riservatezza, adottando tutte le cautele, a non cederlo a terzi e a non consentirne l'utilizzo da parte di terzi, assumendosi la responsabilità di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito di esso, nonché dal suo smarrimento e/o sottrazione. A tal fine il Cliente deve operare con la diligenza e la prudenza che generalmente devono essere osservate da tutti nella cura dei propri interessi patrimoniali.
A titolo esemplificativo e non esaustivo, il Cliente:
- deve conservare il Sistema di Autenticazione in luogo segreto;
- non deve comunicare in alcun modo il Sistema di Autenticazione a terzi;
- deve adottare ogni precauzione volta a mantenere la riservatezza del Sistema di Autenticazione;
- deve verificare con frequenza e costanza le operazioni che risultano compiute attraverso Digital Banking;
- deve fruire di Digital Banking con modalità, device o supporti che si avvalgono di elevati standard di sicurezza;
- deve provvedere a bloccare il Sistema di Autenticazione e/o Digital Banking anche qualora abbia solo il sospetto di utilizzi non autorizzati e/o a fronte di eventuali segnalazioni anche di pericolo da parte della Banca (es. attraverso sms, email o mediante avvisi inviati nell'ambito dei programmi di sicurezza);
- deve adottare soluzioni tecnologiche che proteggono da rischi di frodi (es. software antivirus);
- deve attivare i sistemi e i servizi di sicurezza messi a disposizione da Digital Banking (es. alert);
- deve comunicare alla Banca i propri recapiti aggiornati, ai quali trasmettere informazioni relative agli utilizzi di Digital Banking;
- deve verificare costantemente la presenza nella barra degli indirizzi del corretto acronimo di protocollo "https" (c.d. protocollo di trasferimento ipertestuale, Hyper Text Transfer Protocol), che è utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti che potrebbero essere effettuate tramite attacchi informatici, a differenza di quanto accade nel caso del protocollo di trasferimento "http".

In caso di furto, smarrimento, sottrazione o perdita di riservatezza del Sistema di Autenticazione, nonché di abuso riscontrato o sospetto del servizio, il Cliente dovrà immediatamente comunicarlo alla Banca, contattando il servizio di Assistenza Telefonica o la propria Filiale di riferimento, e provvedere a cambiare la Password utilizzata per fruire di Digital Banking e i recapiti utilizzati per ricevere le Password Monouso, ove necessario. In ogni caso il Cliente dovrà, inoltre, sporgere denuncia di quanto accaduto alle Autorità competenti e trasmetterla alla Banca.
In materia di sicurezza il Cliente potrà consultare l'apposita sezione dedicata alla Sicurezza presente sul sito della Banca. Dal

momento che l'utilizzo di Digital Banking può esporre al rischio di frodi, il Cliente è informato che è suo onere utilizzare i più sofisticati accorgimenti tecnologici tempo per tempo disponibili al fine di evitare che ciò si verifichi ed utilizzare strumenti/servizi che garantiscono elevati standard di sicurezza.

Il Cliente è informato del fatto che, grazie al tempestivo scarico (tramite il salvataggio o la stampa) su supporto duraturo delle comunicazioni inviate da parte della Banca, può evitare il rischio che possa esaurirsi lo spazio della casella postale utilizzata per ricevere le comunicazioni da parte della Banca. È noto, infatti, che nel caso in cui la casella di posta sia piena non è possibile ricevere nuove comunicazioni.

Considerata, inoltre, la complessità e la continua evoluzione dei sistemi di sicurezza e delle tecnologie impiegate in Digital Banking, si deve tenere conto che sussiste una elevata probabilità che i servizi prestati attraverso di esso possano subire interruzioni o sospensioni, e ciò anche senza preavviso del Cliente. Ad esempio, al fine di consentire la verifica della sicurezza, nonché di ogni altro aspetto connesso con l'efficienza e la regolarità di Digital Banking e del Sistema di Autenticazione, il Cliente accetta che la Banca possa, in ogni momento, sospendere a campione Digital Banking, anche in corso di operazione, e rimettere la prosecuzione delle stesse al ricevimento delle conferme del caso. Ne consegue che la fruizione di Digital Banking avviene per libera e consapevole scelta del Cliente, con accettazione del maggior grado di rischio che questa inevitabilmente comporta.

Per l'accesso a Digital Banking mediante dispositivi mobili la Banca mette a disposizione del Cliente delle apposite applicazioni software, contraddistinte dal marchio Banca Monte dei Paschi di Siena, che il Cliente dovrà installare sui propri dispositivi (es. smartphone, tablet). Il Cliente deve utilizzare esclusivamente le applicazioni software "ufficiali" messe a disposizione dalla Banca, fermo restando che l'utilizzo di applicazioni software sviluppate da terze parti non autorizzate dalla Banca non è ammesso per ragioni di sicurezza e il Cliente si assume ogni conseguente responsabilità in caso di violazione del presente divieto. Per le medesime ragioni il Cliente non deve utilizzare siti web, piattaforme informatiche o altre modalità di accesso e utilizzo di Digital Banking se sono forniti da terzi e non sono espressamente ammessi e autorizzati dalla Banca.

Analoghe avvertenze valgono per l'utilizzo degli strumenti di Firma Digitale Remota (FDR) e Posta Elettronica Certificata (PEC). Si segnala, in particolare, che il Cliente:

- deve custodire con la massima cura e diligenza i sistemi di autenticazione che permettono di accedere ai servizi di PEC e FDR, senza cederli a terzi, e preservarne la riservatezza e segretezza, essendo responsabile di ogni conseguenza dannosa derivante dal loro utilizzo;
- deve consultare periodicamente la presenza di nuovi messaggi nella propria casella PEC, posto che in caso di ricezione di messaggi a mezzo PEC è come se si ricevesse una lettera a mezzo raccomandata r.r.;
- deve prestare la massima attenzione nell'utilizzo della FDR, così come quando si trova a firmare di proprio pugno un qualsiasi documento.

Il Cliente potrà rivolgere all'Ente Certificatore accreditato tutte le richieste relative allo svolgimento dei servizi da questo offerti, ivi comprese quelle relative ad eventuali disservizi (ad es. per ritardi, mancati consegne o invii, ecc. …).

LEGENDA

ATM Cardless	L'ATM Cardless è un Canale, fruibile tramite apparecchiature (es. ATM e Cassa Automatica) rese disponibili dalla Banca, accessibile per mezzo del Sistema di Autenticazione e disponibile solo su apparecchiature tecnicamente abilitate.
Banca Telefonica	La Banca Telefonica è un Canale, fruibile tramite apparecchi telefonici ed erogato mediante operatore o risponditore automatico, accessibile per mezzo del Sistema di Autenticazione.
Codice di Conferma	Password monouso numerica inviata al Cliente tramite SMS.
Codice Utente	Codice identificativo, scelto dal Cliente, necessario per accedere ai Canali.
DocumentiOnLine	DocumentiOnLine è un servizio accessorio di Digital Banking che consente al Cliente di ricevere e consultare gratuitamente online le comunicazioni periodiche e specifiche della Banca, comprese quelle previste dalla normativa. I moduli abilitabili a DocumentiOnLine per Rapporto sono disponibili sul sito web www.mps.it.
Firma Digitale Remota	La Firma Digital Remota (FDR) è una tipologia di Firma Digitale accessibile via Internet, nel quale la chiave privata del firmatario viene conservata assieme al certificato di firma da parte di un Ente Certificatore Accreditato.
Internet Banking	L'Internet Banking è un Canale, fruibile tramite un sito web costituito da pagine protette o apposite applicazioni software, accessibili tramite il Sistema di Autenticazione.
Password	Codice segreto, definito dal Cliente, necessario per accedere ai canali telematici.
Posta Elettronica Certficata	La Posta Elettronica Certificata (PEC) è un tipo particolare di posta elettronica, disciplinato dalla Legge italiana, che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale, garantendo così il non ripudio.La Posta Elettronica Certificata (PEC) è un tipo particolare di posta elettronica, disciplinato dalla Legge italiana,

	che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale, garantendo così il non ripudio.
Sistema di Autenticazione	Il Sistema di Autenticazione è l'insieme di processi e strumenti che consentono di verificare a distanza l'identità del Cliente.