MEDIOCREDITO CENTRALE

INVITALIA

N° 10
Decorrenza da 16/03/2021
FI_BDM_CCIMP

Foglio Informativo
Conto Corrente Impresa

INFORMAZIONI SULLA BANCA E SUL SOGGETTO INCARICATO DELL'OFFERTA FUORI SEDE

INFORMAZIONI SULLA BANCA

MEDIOCREDITO CENTRALE S.p.A. (di seguito anche "Banca"), Società con socio unico Invitalia S.p.A., soggetta all'attività di direzione e coordinamento di quest'ultima, codice ABI 10680.7, società per azioni con sede legale in Roma, viale America n. 351, numero di iscrizione all'Albo delle Banche 74762.60 e capogruppo del gruppo bancario Mediocredito Centrale, iscritto all'Albo dei Gruppi Bancari presso la Banca d'Italia con codice ABI 10680, capitale sociale Euro 204.508.690,00 interamente versato, numero di iscrizione al Registro delle imprese di Roma e codice fiscale 00594040586, partita IVA 00915101000, numero REA RM175628, aderente al Fondo Interbancario di Tutela dei Depositi e al Fondo Nazionale di Garanzia di cui all'art. 62, comma1 del D.lgs. n. 23 luglio 1996, n.415, sito internet: www.mcc.it

Dati e qualifica soggetto incaricato dell'offerta fuori sede
Si precisa che il cliente non è tenuto a riconoscere alcun costo od onere al soggetto incaricato dell'offerta fuori sede

Nome e cognome/Ragionesociale_____

Qualifica_____

Sede (indirizzo)_____telefono_____

Email _____ Iscrizione ad Albo/Elenco _____

Numero delibera Iscrizione

CHE COS'È IL CONTO CORRENTE

Il conto corrente è un contratto con il quale la Banca svolge un servizio di cassa per conto del cliente, custodendone il denaro e mantenendolo nella disponibilità dello stesso.
Il conto corrente di Mediocredito Centrale è riservato a clientela "**impresa**", ovvero non consumatori e che al momento dell'apertura svolgeranno un numero limitato di operazioni, ed è in via generale funzionale alla gestione di finanziamenti a breve o medio-lungo termine erogati alla clientela.
Il conto prevede operatività solo in Euro. Il cliente può effettuare e ricevere bonifici SEPA, singoli o ricorrenti, e giroconti. Al conto corrente può essere collegato il servizio di home banking.
L'operatività del conto non comprende la convenzione di assegno né l'emissione di strumenti di pagamento diversi da quanto sopra citato, operatività in contanti né, più in generale, operatività diversa da quanto sopra citato, salvo differenti pattuizioni successive tra le Parti.

Al momento dell'apertura del conto, questo dovrà presentare un saldo minimo pari ad almeno euro mille per eventuali coperture delle spese.

Tra i principali **rischi,** vanno tenuti presenti:

rischio di controparte. Il rischio principale è il rischio di controparte, cioè l'eventualità che la banca non sia in grado di rimborsare al correntista, in tutto o in parte, il saldo disponibile. Per questa ragione la Banca aderisce al Fondo interbancario di tutela dei depositi, che assicura a ciascun correntista una copertura fino a euro 100.000,00;
variazione in senso sfavorevole delle condizioni economiche (tasso di interesse; commissioni e spese del servizio) ove contrattualmente previsto;

smarrimento di dati identificativi e parole chiave per l'accesso al conto su internet, ma sono ridotti al minimo se il correntista osserva le comuni regole di prudenza e attenzione;

estinzione del rapporto e destinazione delle somme dello stesso al Fondo di cui all'art. 1 comma 343 legge 266/2008 in caso in cui il conto non venga movimentato dal/i titolare/i o da terzi da questo delegati, escluso l'intermediario non specificatamente delegato in forma scritta, per almeno 10 anni consecutivi - cd. "Conto dormiente" - (D.P.R. n.116 del 22/06/2007).

PRINCIPALI CONDIZIONI ECONOMICHE

Le voci di spesa riportate nel prospetto che segue rappresentano la gran parte dei costi complessivi sostenuti da un cliente impresa titolare di un conto corrente.
Questo vuol dire che il prospetto non include tutte le voci di costo. Alcune delle voci escluse potrebbero essere importanti in relazione sia al singolo conto sia all'operatività del singolo cliente.
Prima di scegliere e firmare il contratto è quindi necessario leggere attentamente anche la sezione "Altre condizioni economiche".

SPESE FISSE

Voci di Costo	**Importo**
Spese per apertura del conto	€ 0,00
Canone annuo	€ 0,00

MEDIOCREDITO CENTRALE

INVITALIA

Numero di operazioni incluse nel canone annuo	0
Spese annue per il conteggio interessi e competenze	€ 240,00 (€ 60,00 trimestrali)
Invio estratto conto	€ 0,00 formato cartaceo € 0,00 formato elettronico
Periodicità invio estratto conto	Mensile/trimestrale/annuale
Rendicontazione a norma "PSD" (solo per microimprese)	€ 0,00 formato cartaceo € 0,00 formato elettronico
Invio documento di sintesi periodico (nei casi previsti dalla normativa di trasparenza)	€ 0,00 formato cartaceo € 0,00 formato elettronico
Imposta di bollo	Nella misura prevista dalla Legge, attualmente: per persone giuridiche € 100,00 annuale

SPESE VARIABILI

	Voci di Costo	
Gestione Liquidità	Spese unitarie per ogni scrittura relativa a operazioni automatiche e tramite canali telematici (si aggiunge al costo dell'operazione)	€ 0,50
	Spese unitarie per ogni scrittura relativa a operazioni cartacea (si aggiunge al costo dell'operazione)	€ 0,50
Spese di registrazione applicate a tutte le opera che generano righe di e/c	0 €	

INTERESSI SOMME DEPOSITATE

Interessi creditori	Tasso creditore annuo nominale	0,01% al lordo delle imposte vigenti
Capitalizzazione	Periodicità liquidazione interessi creditori	Annuale
	Criterio di capitalizzazione	In base all'anno civile
Ritenuta fiscale		A carico del cliente nella misura pro tempore vigente

SCONFINAMENTI IN ASSENZA DI FIDO

Sconfinamenti in assenza di fido	Tasso debitore annuo nominale sulle somme utilizzate fino a € 1.500,00 oltre € 1.500,00	 21,80% 20,50%
	Commissione di istruttoria veloce	€ 0

Il Tasso Effettivo Globale Medio (TEGM), previsto dall'art. 2 della legge sull'usura (l. n. 108/1996), relativo allo scoperto senza affidamento, può essere consultato sul sito internet della banca (www.mcc.it) e negli appositi prospetti affissi nei locali aperti al pubblico della Banca.

OPERATIVITA' CORRENTE E GESTIONE DELLA LIQUIDITA'

Spese tenuta conto

Spese per duplicato di ogni estratto conto e/c scalare relativo all'anno in corso e ai due precedenti relativo ad anni precedenti gli ultimi tre	 € 3,10 € 7,50
Spese per rilascio certificazioni, dichiarazioni, duplicati e ricerche (costo unitario):	
Attestati per certificazione di bilancio	€ 150,00

MEDIOCREDITO CENTRALE

INVITALIA

Capacità finanziaria	€ 60,00
Capacità finanziaria per Estero	€ 60,00
Lettere liberatorie	€ 30,00
Certificazione rapporti e garanzie	€ 30,00
Competenze liquidate anni precedenti	€ 20,00
Duplicati Copie fotostatiche di documenti	€ 6,50
Informazioni ed accesso dei Clienti a documentazioni, indagini, rilevamenti, constatazioni, ecc.	€ 30,00 per ogni ora occupata dall'impiegato addetto (min. € 15,00)

Servizi di pagamento

BONIFICI IN PARTENZA con addebito in c/c				
Tipologia di bonifico	Conferito su supporto cartaceo		Conferito tramite Home/internet banking	
	Spese fisse	Spese variabili	Spese fisse	Spese variabili
A Bonifico SCT B ricorrente a banche C periodico a banche D stipendi a banche	€ 4,50 € 2,00 € 1,30 € 1,50		€ 1,50 € 1,00 € 0,50 € 1,30	
Bonifico transfrontaliero	€ 4,50	0,25% min. € 2,20 0,25% min. € 2,20	€ 1,50	0,25% min. € 2,20 0,25% min. € 2,20

ALTRE SPESE/COMMISSIONI APPLICATE AI BONIFICI IN PARTENZA	
Disposizioni urgenti (valuta accredito al beneficiario stesso giorno data esecuzione)	€ 15,49
Disposizioni impartite via fax da eseguire stesso giorno, previa pre- autorizzazione della Banca.	€ 25,82
Comunicazione di conferma esecuzione - verso controparte in Italia	€ 4,50
Annullamento del pagamento dopo l 'esecuzione, ma prima della spedizione	€ 10,00
Maggiorazione per bonifici indirizzati a banche non aderenti al circuito SWIFT	€ 10,00

Sconfinamenti.

Tipologia di bonifico	Termini massimi di esecuzione per operazioni disposte entro gli orari di cut off	
1. Bonifico SCT	Con addebito in c/c	Home/Internet banking
A banche Ricorrente a banche Periodico a banche Stipendi a banche	1 gg lavorativi 1 gg lavorativi 1 gg lavorativi 1 gg lavorativi	1 gg lavorativi 1 gg lavorativi 1 gg lavorativi 1 gg lavorativi
Valuta di addebito sul c/c ordinante	Data esecuzione bonifico	

TABELLE DI CUT-OFF			
	OP. SINGOLA SCT	OP. MULTIPLA SCT	HOME BANKING
Giornata operativa	non oltre le 14,00	13,00	13,00
Prefestivi o semi-festivi	non oltre le 10,00	10:00	11,00

Gli ordini disposti dopo i termini temporali previsti dall'Istituto saranno recepiti con data di esecuzione posticipata al primo giorno lavorativo successivo.

Servizi di pagamento

BONIFICI IN ARRIVO (con accredito in C/C)			
Tipologia di bonifico	Spese fisse	Spese variabili	Valuta di accredito
Bonifico SCT	€ 0,00	€ 0,00	Stessa valuta di regolamento

Bonifico transfrontaliero in euro qualsiasi importo	€ 0,00	0,25% minimo € 2,20	2 gg lavorativi successivi alia valuta di regolamento

SERVIZI DI PAGAMENTO	
Spese per comunicazione del rifiuto di un ordine di pagamento giustificato	€ 2,00 + eventuali spese richieste dal prestatore del servizio di pagamento della controparte
Spese per la revoca di un ordine (con mutuo consenso) decorso il termine di irrevocabilità	
Spese per il recupero dei fondi in caso di identificativo unico inesatto	

INTERNET BANKING	
SPESE FISSE	
Canone mensile	€ 10,00
Periodicità addebito canone	Mensile posticipata
SPESE VARIABILI	
Spese produzione /invio documento di sintesi (nei casi previsti dalla normativa di trasparenza)	€ 0,00 invio elettronico € 0,00 invio cartaceo

RECESSO E RECLAMI

Recesso
Si può recedere dal contratto in qualsiasi momento, senza penalità e senza spese di chiusura del conto.

Tempi massimi di chiusura
Si informa il Cliente che l'estinzione di rapporto di conto corrente avverrà entro i tempi massimi di seguito riportati, decorrenti dalla data in cui la richiesta è completa, e valgono soltanto nel caso in cui il saldo da liquidare sia positivo. Di seguito le tempistiche:
- 15 giorni lavorativi dalla data di presentazione della richiesta di estinzione completa da parte del Cliente.
Il perfezionamento della richiesta sarà sospeso qualora, dopo la presentazione della stessa, sopravvengano degli elementi ostativi alla chiusura del conto corrente quali pignoramenti, sequestri, successioni, saldo negativo, etc. In tali ipotesi la Banca provvederà a fornire idonea comunicazione scritta al cliente

Reclami
Nel caso in cui il Cliente intenda presentare un reclamo in relazione all'interpretazione, applicazione ed esecuzione del Contratto, ovvero alle attività preliminari o connesse effettuate, potrà presentarlo a MCC– Ufficio Reclami, anche con lettera raccomandata A/R, tramite mail o PEC, ai seguenti indirizzi:
Ufficio Reclami- MedioCredito Centrale S.p.A., con sede in Viale America, 351 – 00144 Roma - Fax 06 47912784;
e-mail: sectionlegalebanca@mcc.it; PEC: reclami@postacertificata.mcc.it.
La Banca deve rispondere entro 60 (sessanta) giorni, o nel diverso tempo massimo previsto dalla normativa applicabile, dal ricevimento del reclamo stesso, o entro 15 giorni lavorativi qualora il reclamo afferisca servizi di pagamento.

Se il Cliente non è soddisfatto o non ha ricevuto risposta entro il suddetto termine, può rivolgersi all'Arbitro Bancario Finanziario (ABF). Per sapere come rivolgersi all'Arbitro si può consultare il sito www.arbitrobancariofinanziario.it, chiedere presso le Filiali della Banca d'Italia, oppure chiedere alla Banca. La decisione dell'Arbitro non pregiudica la possibilità per il Cliente di ricorrere all'autorità giudiziaria ordinaria; in tal caso lo stesso non sarà tenuto ad esperire il procedimento di mediazione di cui al successivo capoverso.

Sempre ai fini della risoluzione delle controversie che possano sorgere e in relazione all'obbligo previsto dal decreto legislativo 4 marzo 2010 n. 28, così come modificato dal D.L 21 giugno 2013, n. 69, convertito in Legge n.98 del 9 agosto 2013, di esperire il procedimento di mediazione, in quanto condizione di procedibilità, prima di presentare ricorso all'autorità giudiziaria, la Parte Mutuataria e/o gli eventuali garanti e la Banca possono ricorrere all'Organismo di Conciliazione Bancaria costituito dal Conciliatore Bancario Finanziario - Associazione per la soluzione delle controversie bancarie, finanziarie e societarie - ADR (www.conciliatorebancario.it dove è consultabile anche il relativo Regolamento) oppure ad uno degli altri organismi di mediazione, specializzati in materia bancaria e finanziaria, iscritti nell'apposito registro tenuto dal Ministero della Giustizia.

MEDIOCREDITO CENTRALE

INVITALIA

LEGENDA	
Canone annuo	Spese fisse per la gestione del conto.
Commissione di istruttoria veloce	Commissione determinata in misura fissa e commisurata ai costi sostenuti per la valutazione creditizia (istruttoria veloce) necessaria ad autorizzare l'operazione. Viene applicata in caso di addebiti che determinano, rispetto al saldo disponibile di fine giornata, uno sconfinamento o accrescono uno sconfinamento già esistente. La commissione non è dovuta quando lo sconfinamento ha luogo per effettuare un pagamento a favore della Banca, o se la Banca non ha autorizzato lo sconfinamento.
Disponibilità somme accreditate	Numero di giorni successivi alia data dell'operazione dopo i quali il cliente può utilizzare le somme accreditate.
Saldo disponibile	Somma disponibile sul conto, che il correntista può utilizzare.
Sconfinamento in assenza di fido	Somma che la banca ha accettato di pagare in caso di addebito sul conto corrente di somme senza che vi sia la disponibilità.
Spese unitarie per ogni scrittura	Spesa per la registrazione contabile di ogni operazione oltre quelle eventualmente comprese nel canone annuo.
Spese annue per conteggio interessi e competenze	Spese per il conteggio periodico degli interessi, creditori e debitori, e per il calcolo delle competenze.
Spese per invio estratto conto	Commissioni che la banca applica ogni volta che invia un estratto conto, secondo la periodicità e il canale di comunicazione stabiliti nel contratto.
Tasso creditore annuo nominale	Tasso annuo utilizzato per calcolare periodicamente gli interessi sulle somme depositate (interessi creditori), che sono poi accreditati sul conto, al netto delle ritenute fiscali.
Tasso debitore annuo nominale	Tasso annuo utilizzato per calcolare periodicamente gli interessi a carico del cliente sulle somme utilizzate in relazione allo sconfinamento.
Valute sui bonifici addebitati	Numero dei giorni che intercorrono tra la data del bonifico addebitato e la data dalla quale iniziano ad essere addebitati gli interessi. Quest'ultima potrebbe anche essere precedente alia data del bonifico addebitato.
Valute sui bonifici accreditati	Numero dei giorni che intercorrono tra la data del bonifico e la data dalla quale iniziano ad essere accreditati gli interessi.

MEDIOCREDITO CENTRALE

INVITALIA

18/9/2019

Corporate banking – Servizio InBank: informazioni per l'esecuzione in sicurezza di operazioni di pagamento via internet

Premessa

L'applicativo di Corporate banking (Servizio InBank), a mezzo della rete Internet, permette di effettuare operazioni di pagamento o avere informazioni sui rapporti di conto corrente che il Cliente intrattiene con la Banca. Il documento riporta le informazioni operative utili per l'uso dell'applicativo e alcuni suggerimenti e regole di sicurezza informatica che il Cliente dovrebbe seguire per ridurre i pericoli insiti nella navigazione tramite rete Internet.

Accesso al Servizio InBank e autenticazione dell'utente

Il servizio InBank funziona attraverso la rete internet. La Banca fornisce al Cliente l'indirizzo del servizio nella rete Internet, accessibile tramite web browser.
L'accesso è possibile utilizzando qualunque provider.

Il Servizio InBank adotta l'autenticazione forte tramite procedura Secure call.

La procedura Secure call prevede l'autenticazione tramite:

- ✓ credenziali personali di accesso (codice cliente/username e password)
- ✓ collegamento telefonico con il Cliente, dal numero di cellulare registrato in contratto al numero verde fornito dal servizio In Bank, e digitazione sulla tastiera del telefono del codice presentato in apposita videata.

La banca fornisce al Cliente, tramite SMS ed email ai recapiti forniti dal Cliente, le credenziali personali di accesso. Al primo accesso il Cliente dovrà modificare la password comunicata dalla Banca per il primo accesso.
Ai fini dell'identificazione, la procedura Secure Call verifica il corretto abbinamento cliente/codice/numero di cellulare.

Per l'effettuazione di una disposizione di pagamento elettronico, oltre a quanto previsto per l'autenticazione occorre:

- ✓ digitare sulla tastiera del cellulare un secondo codice generato dall'applicazione (Dynamic link). Se le cifre digitate corrisponderanno a quanto presentato a video, la disposizione sarà autorizzata.

L'uso congiunto del codice cliente (username), della password segreta, del codice generato dal sistema Secure call e dell'ulteriore codice generato in caso di disposizione di pagamento (di seguito codici) autorizza l'esecuzione della disposizione di pagamento.

Suggerimenti per la corretta gestione delle credenziali di accesso

Per difendersi da:

- *Furto d'identità,*
- *Accesso non autorizzato.*

La sottrazione di una password può avere importanti impatti personali e organizzativi: un malintenzionato che utilizza credenziali rubate è abilitato ad eseguire azioni dannose la cui responsabilità può ricadere sul titolare dell'identità digitale.
A tal proposito, l'uso di una password "robusta" è il primo elemento che garantisce una difesa dagli accessi non autorizzati e la protezione dei dati.
Nel caso si sbagli per più di tre volte la password, l'applicativo blocca per sicurezza l'utenza. In questo caso è necessario contattare il supporto tecnico (vedi capitolo successivo) per chiederne la riattivazione.

- ➢ Scegliere una password di almeno 8 caratteri e che contenga sia numeri che lettere maiuscole e minuscole. Se il sistema di autenticazione lo permette utilizzare anche caratteri speciali, quali "$", "&", "%", "#",
- ➢ Non usare la stessa password per accedere a diversi sistemi. Evitare assolutamente l'uso della stessa password per applicazioni personali e applicazioni aziendali,
- ➢ Non comunicare le password a terzi,
- ➢ Non conservare le password in luoghi facilmente accessibili,
- ➢ Evitare che la password sia visibile sullo schermo durante la digitazione,
- ➢ Cambiare periodicamente la password,

- Evitare strumenti di memorizzazione delle password, soprattutto su sistemi critici che abilitano alla consultazione e modifica di dati.

Descrizione della procedura di autorizzazione e/o informazione

Accesso al sistema:
Il Cliente in fase di autenticazione al sistema utilizzerà il sistema standard inserendo username e password.
Successivamente all'inserimento delle prime credenziali (primo fattore), l'applicazione chiederà se si vuole essere chiamati (domanda "Sono all'estero") o se si vuole chiamare il numero verde. Con la chiamata telefonica (effettuata dal sistema o dal cliente) il *Secure call*:

1) Richiederà di inserire il codice presentato in apposita videata dell'applicazione di Corporate banking.
2) Verificherà il corretto abbinamento cliente/codice/numero di cellulare. In caso di esito positivo l'azione sospesa sul Corporate banking sarà autorizzata.

Esempio di Accesso al sistema:

Fase 1:

- Inserire nel campo "Codice Postazione" il proprio codice cliente/username
- Inserire nel campo "Password di accesso" la password
- Selezionare il bottone "Accedi"

Fase 2:

- Tenere a portata di mano il Telefono Cellulare il cui numero è dichiarato nel contratto
- Selezionare il bottone "Accedi"

MEDIOCREDITO CENTRALE

INVITALIA

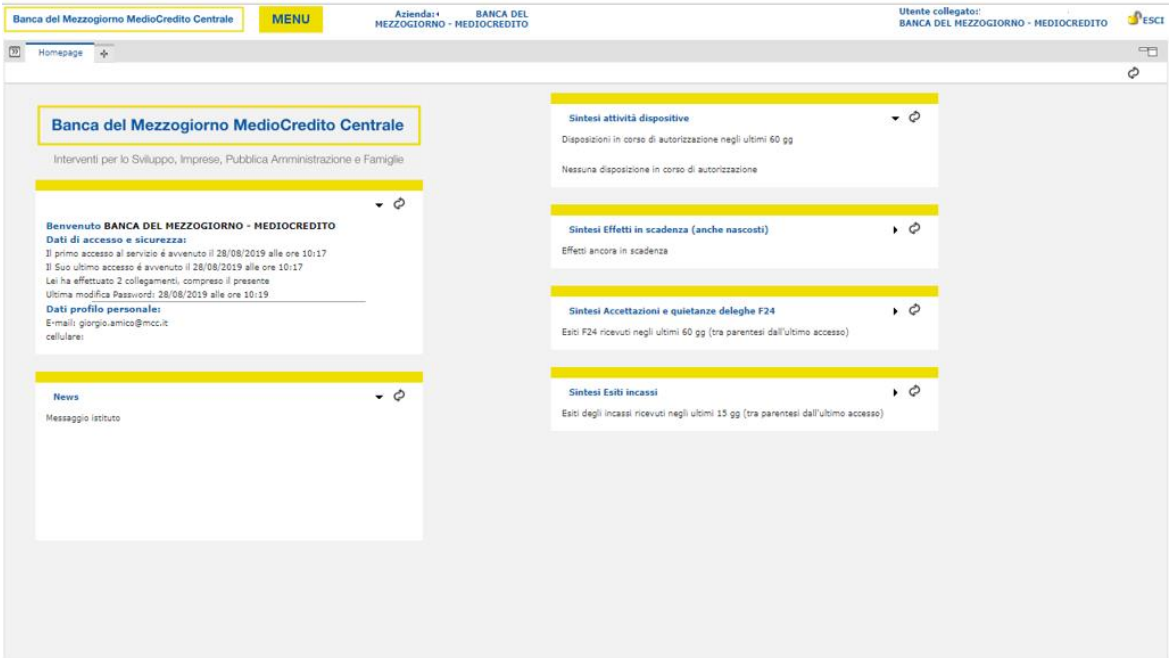
Fase 3:
Successivamente all'inserimento delle prime credenziali (primo fattore), l'applicazione chiederà se si vuole essere chiamati (domanda "Sono all'estero") o se si vuole chiamare il numero verde. Con la chiamata telefonica (effettuata dal sistema o dal Cliente) il *Secure call* procederà con le fasi di autenticazione successive.

Fase 4:

- Con il Telefono Cellulare il cui numero è dichiarato nel contratto, comporre il numero indicato alla voce "Chiamare dal cellulare abilitato il seguente numero" o attendere la chiamata del Secure call (a seconda della scelta effettuata nella fase precedente).
- Il Secure call richiede di inserire sulla tastiera del telefono cellulare il codice riportato alla voce "Inserire il seguente codice seguendo il messaggio"

Fine processo

Conclusa la fase di Autenticazione viene visualizzata la pagina Home del "Corporate Banking"



Autorizzazione di una disposizione o distinta di pagamento

In fase di autorizzazione di un'operazione dispositiva (singolo bonifico o distinta di pagamento), si procederà come segue:

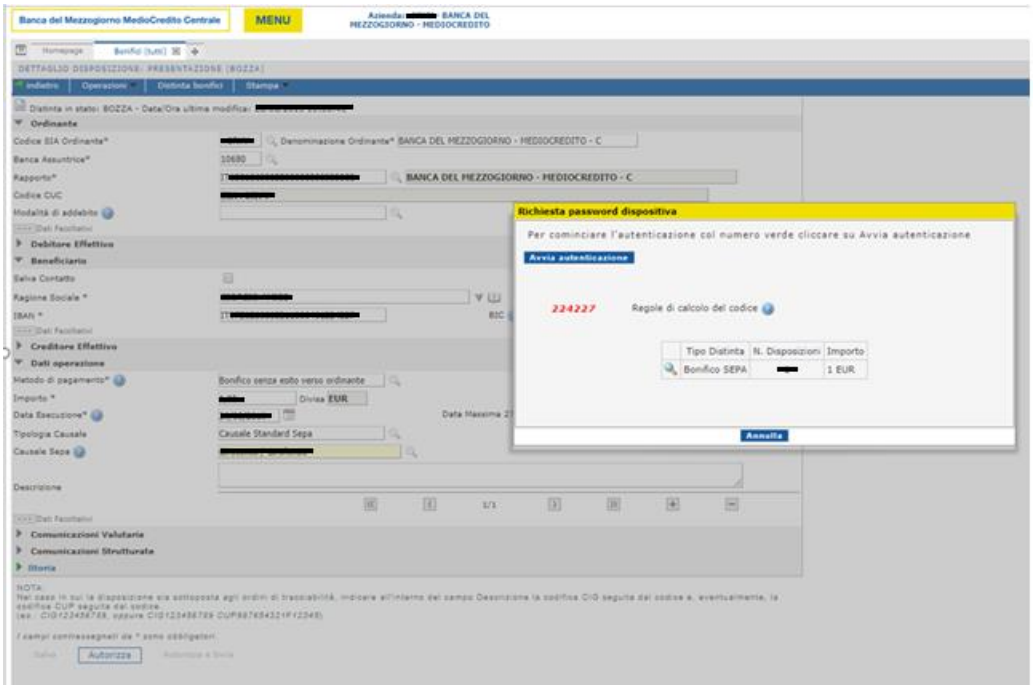
1) Il Sistema chiederà, in apposita videata, se si vuole essere chiamati (domanda "Sono all'estero") o se si vuole chiamare il numero verde. A secondo della scelta, verrà attivata una comunicazione telefonica.
2) Il Sistema visualizzerà una schermata con:
   a) il riepilogo delle informazioni inserite in fase di disposizione di pagamento, in particolare importo da pagare e l'IBAN di accredito.
   b) Il primo codice,
   c) le cifre generate dall'applicazione (Dynamic link).
3) Una voce automatica richiederà di inserire il codice e il Secure call verificherà il corretto abbinamento codice cliente/codice /numero di cellulare. In caso di esito positivo si procederà con il passo successivo
4) Autorizzazione tramite Dynamic link: viene richiesto di digitare sulla tastiera del cellulare le cifre generate dall'applicazione. Se le cifre digitate corrisponderanno a quanto presentato a video, l'azione sospesa sul Corporate banking sarà autorizzata.

Esempio di Autorizzazione di una disposizione o distinta di pagamento:

Fase 1:

Con l'azione di "Autorizza" che l'utente effettua dopo aver predisposto la disposizione (es. bonifico) o distinta di pagamento il Secure call presenterà una finestra (Pop-up) "Richiesta password dispositiva" attraverso la quale si può:

- Annullare l'operazione selezionando il bottone "Annulla"
- Proseguire con l'operazione selezionando il bottone "Avvia autenticazione"

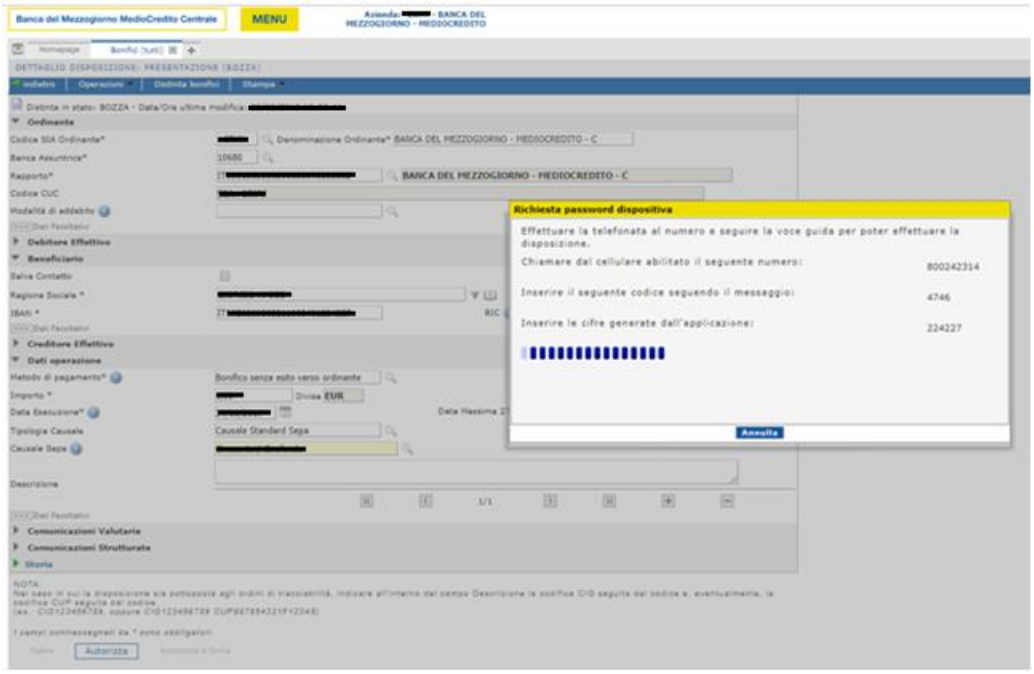


Fase 2:

Successivamente all'inserimento delle prime credenziali (primo fattore), l'applicazione chiederà se si vuole essere chiamati (domanda "Sono all'estero") o se si vuole chiamare il numero verde. Con la chiamata telefonica (effettuata dal sistema o dal cliente) il *Secure call* procederà con le fasi di autenticazione successive.

Fase 3:

- Con il Telefono Cellulare il cui numero è dichiarato nel contratto, comporre il numero indicato alla voce "Chiamare dal cellulare abilitato il seguente numero" o attendere la chiamata del Secure call (a seconda della scelta effettuata nella fase precedente).
- Il Secure call richiede di inserire sulla tastiera del telefono cellulare il codice riportato alla voce "Inserire il seguente codice seguendo il messaggio"
- A seguire, il Secure call richiede inserire sulla tastiera del telefono cellulare il codice riportato alla voce "Inserire le cifre generate dall'applicazione"
- il Secure call verificherà il corretto abbinamento codice cliente/codice /Cifre generate dall'applicazione/numero di cellulare. In caso di esito positivo la transazione sarà autorizzata.



Orientamenti per l'uso corretto e sicuro dell'hardware e il software

Per difendersi da:

- *Furto d'identità,*
- *Furto del dispositivo,*
- *Perdita o alterazione delle informazioni,*
- *Compromissione del dispositivo*.

- Se ci si allontana dal computer, bloccarlo tramite i tasti "Ctrl+Alt+Canc" (oppure tasto Win+L). Al nuovo accesso sarà richiesta la password Windows.
- Attivare in modo automatico lo screen saver dopo 5 minuti. Riattivando il dispositivo si deve ritornare alla videata di accesso Windows che richiede obbligatoriamente la password Windows.
- Evitare di lasciare il computer o il cellulare incustodito se ci si trova in locali pubblici o, in generale, dove non si ha il controllo degli accessi.
- Per ridurre il rischio di malfunzionamento del computer o del cellulare, con possibile perdita dei dati, in prossimità dei dispositivi evitare l'uso di liquidi o sostanze/oggetti che possono recare un danno all'hardware.

Precauzioni nell'uso della rete Internet

Per difendersi da:

- *Furto d'identità,*
- *Accesso non autorizzato,*
- *Perdita di informazioni,*
- *Codice malevolo.*

Ci sono diverse infrastrutture tecniche per ridurre i rischi che si possono avere lavorando su rete pubblica, quali ad es. firewall, antivirus, antispam. E' importante proteggere i dispositivi con i quali si accede alla rete internet con tali infrastrutture, e mantenerle aggiornate.

Talvolta questi strumenti possono non essere sufficienti a garantire la sicurezza della navigazione Internet.

Prestare massima attenzione al mittente delle mail (soprattutto se non conosciuto), all'oggetto, al contenuto e ai link o allegati.

Casi di potenziali mail malevole:

- Errori linguistici grossolani nell'oggetto o nel testo;
- Il dominio di rete non è noto o palesemente contraffatto;
- Presenza di link che puntano a siti web sconosciuti o contraffatti. Particolarmente pericolosi sono i link che rimandano a pagine web che richiedono credenziali di accesso;
- Prestare attenzione se l'oggetto della mail riporta i caratteri "I:", "R:", "RE:", "Frw:". Questi caratteri indicano una mail di risposta ad una vostra precedente mail. Sono espedienti usati nelle mail malevole per ingannare il destinatario ed indurlo a pensare che si tratti di una risposta ad una sua mail.

Il download di file da Internet può nascondere codice malevolo. Anche disponendo di un antivirus, questo potrebbe non essere in grado di rilevare il codice malevolo perché non noto o non ancora rilevabile.

Effettuare il download solo da fonti attendibili e/o conosciute.

Se tramite browser Internet si stanno trattando dati sensibili o riservati accertarsi che l'indirizzo web su cui si sta lavorando inizi con "https://". HTTPS è un protocollo di comunicazione sicuro che garantisce la non intercettazione dei dati trasferito tra client e server. Si può controllare da browser la certificazione rilasciata al proprietario del sito contattato.

Protezione dei propri dati

Per difendersi da:

- *Perdita di riservatezza,*
- *Perdita dei dati.*

- Effettuare periodicamente un backup (copia di sicurezza):
  - Utilizzare un hard disk esterno oppure una chiavetta usb,
  - La copia si effettua tramite i comandi Windows di copia/incolla,
  - Se i documenti/dati sono appoggiati su spazi del server aziendale o su Cloud, non è necessario effettuare il backup (viene effettuato automaticamente dal Servizio IT o dall'azienda che gestisce l'area di archiviazione Cloud),
- La copia di sicurezza (backup) deve essere custodita in postazione sicura e sotto il controllo del proprietario. È necessario che sia protetta con un sistema di cifratura perché questo garantisce l'accesso al solo proprietario,
- Utilizzare un sistema di cifratura. Ne esistono diversi, anche preinstallati nel sistema operativo.

Utilizzo di supporti rimuovibili

Per difendersi da:

- *Codice malevolo*[1]*,*
- *Perdita dei dati.*

L'uso di dispositivi rimovibili (es. chiavette USB), può essere causa di propagazione di codice malevolo (virus informatico). Tali dispositivi sono inoltre a rischio di perdita o furto.

- Riporre sempre in luoghi sicuri e sotto il proprio diretto controllo i supporti rimovibili,
- Se si collegano supporti rimovibili provenienti da fonti non conosciute o affidabili, provvedere ad effettuare una preliminare scansione antivirus.

Accesso alle reti

Per difendersi da:

- *Intercettazioni del traffico dati (cosiddetto "man in the middle"),*
- *Riservatezza dei dati.*

[1] La dizione "malevolo" è volutamente generica perché comprende varie tecniche di attacco che hanno nomi diversi. I nomi più usati sono "virus informatici", worm, trojan, rootkit, spyware, malware, ransomware. Sono tutte tipologie di codice malevolo che agisce o si diffonde in modo differente.

Se si effettua la connessione a Internet dal sistema aziendale, il traffico su rete pubblica (Internet) dovrebbe essere adeguatamente protetto; verificare chiedendo informazioni al vostro Servizio IT.
Se si effettua la connessione a Internet al di fuori del sistema aziendale, si potrebbero utilizzare reti Wi-Fi cosiddette "aperte". Le reti "aperte" sono reti pubbliche in cui il traffico delle informazioni non è protetto in alcun modo. Sono reti aperte quelle disponibili in luoghi pubblici, bar, centri commerciali, alberghi, dove chiunque si può collegare; il sistema non conosce e non controlla i computer che sono collegati a tali reti.
Si riconosce una rete aperta dal fatto che non è necessario autenticarsi con una username e password personale. Il collegamento è possibile a volte senza alcuna password, spesso con una password unica per tutti i computer. Le informazioni che transitano su reti "aperte" sono facilmente monitorabili e accessibili da parte di terzi connessi alla medesima rete.
Se è necessaria una connessione a reti aperte evitare di trasmettere dati aziendali.

Procedure da seguire in caso di perdita o furto delle credenziali di sicurezza o dell'hardware o del software per l'accesso o l'esecuzione delle operazioni o in caso di abuso riscontrato o sospetto

In caso di perdita o furto delle credenziali personali di accesso o in caso di utilizzo indebito o non autorizzato, sottrazione o smarrimento del dispositivo personale abilitato alla procedura Secure Call, il Cliente deve chiamare immediatamente il numero **800 938 375.**
La Banca provvederà a disattivare i codici nel più breve tempo possibile e comunque entro 1 giorno lavorativo dal ricevimento della comunicazione. Tempestivamente, il Cliente si impegna a confermare per iscritto (anche a mezzo fax) alla Banca le medesime informazioni e, in caso di smarrimento o sottrazione del dispositivo, a farne denuncia all'Autorità Giudiziaria o di Polizia.
Il Cliente può richiedere il ripristino del proprio codice di accesso (password iniziale) nonché la riattivazione del Servizio InBank in caso di blocco, laddove siano venute meno le ragioni che ne hanno comportato e la Banca non abbia già provveduto alla riattivazione.
Inoltre, il Cliente deve comunicare alla Banca la variazione del numero di cellulare e/o dell'indirizzo di posta elettronica certificata comunicati in contratto ed utilizzati per la procedura di Secure Call e/o per le comunicazioni relative all'esecuzione del Servizio.

In ogni caso, **la Banca si riserva la facoltà di bloccare l'utilizzo del Servizio InBank** – ed eventualmente operazioni in corso di esecuzione – **per giustificati motivi connessi alla sicurezza del sistema e/o al sospetto di un utilizzo fraudolento o non autorizzato dello stesso**.

In tal caso la Banca informa il Cliente del blocco del Servizio InBank, motivando tale decisione, tramite telefonata registrata o via posta elettronica certificata agli ultimi recapiti forniti con le modalità contrattualmente previste e provvede a riattivare il Servizio – e all'esecuzione delle operazioni di pagamento sospese - al venir meno delle ragioni che ne hanno comportato il blocco.

Responsabilità e oneri della Banca e del Cliente nell'uso del Servizio InBank

Responsabilità della Banca

- La Banca è responsabile nei confronti del Cliente della corretta esecuzione dell'ordine di pagamento ricevuto.
- Qualora il Cliente sia venuto a conoscenza di un'operazione di pagamento non autorizzata o non correttamente eseguita, ivi compresi i casi di mancata, inesatta o tardiva esecuzione, ha il diritto di ottenerne la rettifica solo se comunica tale circostanza alla Banca, scrivendo all'indirizzo email SistemiPagamentoMCC@mcc.it, senza indugio e comunque entro 13 mesi dalla data di addebito del Conto, nel caso di Cliente ordinante, o dalla data di accredito nel caso di Cliente beneficiante.
- Nel caso in cui sia stata eseguita un'operazione di pagamento non autorizzata o l'operazione sia stata eseguita in modo inesatto, la Banca rimborsa al Cliente l'importo dell'operazione medesima immediatamente o, al più tardi, entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione ovvero riceve una comunicazione in merito, riportando il conto allo stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo e assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo dell'operazione non autorizzata sul conto. La Banca è inoltre responsabile nei confronti del Cliente di tutte le spese ed interessi imputati a seguito della mancata, inesatta o tardiva esecuzione dell'operazione di pagamento.

- La Banca può sospendere il rimborso in caso di motivato sospetto di frode.
- L'obbligo di rimborso non si applica se la Banca dimostra che il prestatore di servizi di pagamento del beneficiario ha ricevuto l'importo dell'operazione, anche se con lieve ritardo. In questo caso il prestatore di servizi di pagamento del beneficiario accredita l'importo al proprio utente con data valuta non successiva a quella che gli sarebbe stata attribuita in caso di esecuzione corretta.

Responsabilità del Cliente

- Salvo il caso in cui abbia agito in modo fraudolento, il Cliente non sopporta alcuna perdita derivante dall'utilizzo delle credenziali personali di accesso e/o del dispositivo personale abilitato alla procedura Secure call indebitamente intervenuto dopo aver comunicato alla Banca la perdita o furto delle credenziali personali di accesso o l'utilizzo indebito o non autorizzato, sottrazione o smarrimento del dispositivo personale.
- Salvo il caso in cui abbia agito in modo fraudolento, il Cliente non è responsabile delle perdite derivanti dall'utilizzo delle credenziali personali di accesso e/o del dispositivo personale abilitato alla procedura Secure call smarriti, sottratti o utilizzati indebitamente quando la Banca non ha adempiuto all'obbligo di assicurare che siano sempre disponibili strumenti adeguati affinchè il Cliente possa eseguire la comunicazione di cui sopra.
- Salvo il caso in cui abbia agito in modo fraudolento, il Cliente non sopporta alcuna perdita se la Banca non esige un'autenticazione forte.
- Il Cliente non sopporta alcuna perdita se lo smarrimento, la sottrazione o l'appropriazione indebita delle credenziali personali di accesso e/o del dispositivo personale abilitato alla procedura Secure call non potevano essere notati dallo stesso prima di un pagamento, salvo il caso in cui abbia agito in modo fraudolento, o se la perdita è stata causata da atti o omissioni di dipendenti della Banca.
- Negli altri casi, salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi contrattualmente previsti con dolo o colpa grave, il Cliente può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito delle credenziali personali di accesso e/o del dispositivo personale abilitato alla procedura Secure call, conseguente al furto, smarrimento o appropriazione indebita degli stessi.
- Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più degli obblighi contrattualmente previsti con dolo o colpa grave, il Cliente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro.

Le responsabilità di cui sopra possono essere derogate qualora il Cliente non sia una micro-impresa.