**DESCRIEREA FUNCTIONALĂ**

**a Sistemului de deservire bancară la distantă**

**„MICB Mobile - Business”**

1. **Prevederi generale**
   1. Prezentul document reprezintă o descriere succintă a Sistemului de deservire bancară la distanță a clienţilor B.C. „Moldindconbank” S.A (în continuare Băncii).

1.2 **MICB Mobile-Business** este disponibil împreună cu sistemul MICB Web-Business în cadrul unui pachet digital a servicilor Moldindconbank la distanţă. Sistemul este o parte componentă a sistemului “MICB Web-Business” şi nu poate utilizat fără conectare la sistemul “MICB Web-Business”. Aplicatiile Web și Mobile identificate prin autentificarea utilizatorilor printr-un singur login.

Sistemul MICB Web-Business şi MICB Mobile-Business prezintă părți componente din cadrul sistemului Qsystems.WebClient.

Banca acordă servicii MICB Mobile-Business, în baza Contractului de prestare a serviciilor de plăţi electronice la distantă (sistemul „MICB Web-Business”)

MICB Mobile-Business este elaborat de compania Qsystems S.R.L. în anul 2014 şi implementat de către BC Moldindconbank SA în 2015.

1.3 **MICB Mobile-Business** reprezintă sistema de tip “Mobile-banking” care oferă Abonatului servicii atât informaţionale, cât și tranzacţionale.

Sistema permite clienților accesul în regim online, la următoarea informație: soldul în cont, istoria tranzacţiilor efectuate pe o anumită perioadă şi confirmarea documentelor create în sistema "MICB Web-Business".

Aceasta sistema permite clientului să controleze şi să gestioneze resursele sale financiare, din Bancă, folosind telefoanele mobile, tabletele.

Aplicaţia **MICB Mobile-Business** este disponibilă prin **AppStore**, **GooglePlay, MarketPlace** (în continuare Market digital) în funcţie de sistemul de operare a dispozitivului mobil (smartphone, tabletă), şi poate fi descărcată gratuit.

1. **Noțiunile utilizate**

**„MICB Mobile - Business”** este parte componentă a sistemului MICB Web - Business, ce funcţionează pe baza sistemelor de operare Android ,IOS si WindowsMobile. Serveşte pentru vizualizarea **cursului BNM,** listei conturilor şi a extrasului pe o perioadă la alegere şi pentru vizualizarea documentelor spre semnare cu ajutorul Semnăturii mobile.

* **Bancă** – proprietarul Sistemului: BC „Moldindconbank” S.A.
* **Abonat** – Clientul care este abonat la Sistem.
* **Client** - SBDD (client conectat la sistemul bancar de deservire la distanţă) - un client al băncii (persoană juridică), care în baza contractului semnat cu banca deţine rechizitele de autentificare în sistemul MICB Web – Business.
* **Abonament** – totalitatea relaţiilor reglementate dintre Abonat şi Bancă aferente Sistemului, precum şi înregistrarea parametrilor şi statutului acestei relaţii.
* **Abonare la Sistem** – procesul în urma căruia Clientul obţine calitatea de Abonat în sensul prezentelor Ghid de utilizare MICB Mobile-Business, se stabileşte Abonamentul şi Banca îi alocă Clientului Loghinul şi Parola.
* **Aplicaţia Mobilă „MICB Mobile Business”** –aplicaţia este accesibilă pentru sistemele de operare **iOS 4** şi mai avansat; **Android 4.2.2** şi mai avansat; **Windows Mobile 8.5.**
* **Dispozitivul mobil (al Abonatului) –** echipament de tip, smartphone sau tabletă, utilizat de către Abonat pentru conectarea la Sistem și utilizarea ulterioară a acestuia.
* **Loghin** – identificator alfanumeric alocat de Bancă Clientului pentru identificarea Clientului în calitate de Abonat.
* **Parolă** – identificator alfanumeric alocat de Bancă Clientului sau stabilit de către Client în procesul de Abonare sau modificat ulterior de către Abonat în cardul Sesiunii de utilizare a sistemului, procedură necesară pentru Autentificarea Clientului în Sistem în calitate de Abonat.
* **Semnatura mobilă -**- se foloseşte pentru semnarea oricăror documente electronice. Semnătura mobilă reprezintă un eşantion de date ce demonstrează că o anumită persoană a scris sau a fost de acord cu acel

document căruia i s-a ataşat o semnătură. Semnătura mobilă permite autentificarea mesajelor/documentelor electronice, asigurînd identitatea expeditorului şi a destinatarul; şi integritatea mesajului /documentului. Conectarea la semnătura mobilă se execută de către operatorul telefoniei mobile Moldcell/ Orange prin substituirea cartelei SIM existente cu o alta cartelă SIM care deţine semnătura digitală.

* **Document electronic** – orice document verificat şi transmis Băncii de către Abonat prin intermediul Sistemului.

1. **Instalarea sistemului**

Prin Market digital se caută aplicația mobilă după abrevierea “MICB”. Din rezultatele căutării se alege “MICB Mobile Business” și se lansează instalarea. Instalarea aplicației este gratuită.

**4. Funcţiile Sistemului**

4**.1** Serviciile non-financiare ale Sistemului sunt alte Servicii decât cele destinate creării şi transmiterii în adresa Băncii a Documentelor electronice de plată.

**4.2 Serviciile informaţionale:**

**4.2.1** Posibilitatea vizualizării cursului valutar.

**4.2.2** Oferă abonatului informații referitor la lista conturilor şi vizualizarea extraselor din conturi (lei, valuta):

* din ziua precedentă;
* din ultima săptămînă;
* pe o altă perioada.

**4.2.3** Oferă posibilitate abonatului să vizualizeze listele cu documente spre semnare:

* transfer de credit în lei moldovenești de tip 001;
* transfer de credit în lei moldovenești de tip 101(dispoziţie de plată trezorerială);
* transfer de credit în valută;
* transfer interbancar în valută;
* cerere de cumpărare / vânzare / convertire a valutei;

Confirmarea documentelor se efectuează prin semnătura digitală.(Semnătura mobilă)

Sistemul nu permite crea documente de plată.

**5. Abonarea la Sistem**

Pentru accesarea aplicaţiei **MICB Mobile-Business** este necesar de indicat Loghinul şi parola. Se utilizează același cont și parola ca și în cazul accesului la sistemul ”MICB Web Business”.

* În cazul în care este disponibil loghin-ul şi parola personală (din 16 simboluri) utilizată pentru accesul în sistemul WebClient (versiunea anterioară), se intră în sistem (<https://web.micb.md/Bol.WebBusiness>) cu parola veche şi în rubrica **ADMINISTRARE** se alege **SCHIMBAREA PAROLEI MELE** după care se modifică parola. Cu parola nouă puteţi accesa aplicaţiile **MICB Web-Business** şi (<https://web1.micb.md/>) **MICB Mobile-Business.**
* Interfaţa nouă a sistemului **MICB Web-Business** este disponibilă la accesarea prin intermediul următoarelor browsere: **Google Chrom, Mozilla FireFox, IExplorer v11** sau **Safari**.
* În cazul în care nu este disponibil loghin şi parola personală de acces, este necesar să fie încheiat un contract de deservire cu Bancă.

Instrucțiuni detaliate de instalare și utilizare sunt descrise în documentul Ghid de utilizare MICB Mobile-Business.

1. **Cerințele tehnice**

Clienții pot accesa aplicația utilizînd următoarele sisteme de operare **iOS 4** şi mai avansat; **Android 4.2.2** şi mai avansat; **WindowsMobile8.5**.

Aplicația WEB a sistemului „MICB Web-Business” <https://web1.micb.md/> este localizată pe serverul băncii.

Procedura de obținere a extrasului folosește serviciului web intern, activarea căruia se execută de către client prin accesarea aplicației Web.

1. **Semnătura mobilă**

Centrul de Telecomunicații Speciale (CTS), în baza contractului încheiat, oferă Băncii posibilitatea aplicării semnăturii digitale folosind **Semnătura mobila.**

Fiecare utilizator pentru a se abona la **Semnatura mobila** completează Anexa 6 a Contractului de prestare a serviciilor de plăţi electronice la distantă (sistemul „MICB Web-Business”) indicînd numărul de telefon mobil, la care va fi expediat o cerere pentru o semnătura digitală.

**8. Mișcarea fluxurilor de informații**

Accesul aplicației mobile la resursele bancare se efectuează prin intermediul aplicației web <https://web1.micb.md/BOL.WebClientTT>

**8.1. Verificarea soldului in cont**

După accesarea reușita a sistemei de către utilizator, aplicația mobilă va afișa pe ecranul dispozitivului mobil lista conturilor clientului (în conformitate cu drepturile de acces) şi va relata soldul contului. Procesul obținerii soldului activează următoarele funcții:

- verificarea accesului utilizatorilor;

- obținerea listei conturilor accesibile;

Pentru fiecare cont:

- formarea cererii către serviciul Web;

- serviciul Web execută o cerere către procedurile relevante din baza de date SAB;

- obținerea răspunsului de la serviciul Web;

- afișarea soldurilor.

**8.2. Obținerea extrasului**

Pe ecranul dispozitivului mobil se selectează contul.

Pe următorul ecran se alege perioada necesară (data curentă, săptămâna trecuta sau o altă perioadă).

Procesul obținerii extrasului activează următoarele funcții:

- verifică accesul utilizatorului;

- formează cerere către serviciul web;

- serviciul Web execută o cerere către procedurile relevante din baza de date SAB;

- obținerea răspunsului de la serviciul Web;

- afișarea extrasului.

**8.3. Confirmarea plaților**

Din meniu se alege punctul “Pentru semnare”:

* Pe ecran se afișează lista documentelor disponibile pentru a fi acceptate prin intermediul semnăturii digitale.
* Este necesar de marcat documentele care urmează a fi semnate şi se apasă butonul “Semnează”. Sistema formează un pachet cu documentele selectate şi indică codul pachetului, suma totală si numărul de telefon al utilizatorului.
* Semnarea documentelor de plată din sistemul ”MICB Mobile Business” poate fi efectuată doar de dispozitivele mobile ce dețin Semnătura mobilă.
* CTS expediază o cerere către utilizatorul de telefonie mobila corespunzător (Moldcell/Orange), operatorul mobil expediază o cerere către numărul de telefon corespunzător.
* La telefonul mobil al utilizatorului, la primirea cererii de la operatorul mobil, se lansează o aplicație specială din cartela SIM, care informează despre o nouă solicitare de semnătura, indică informația despre pachet (numărul tranzacției, numărul de documente, suma) şi solicită codul PIN pentru accesul la certificat, situat pe cartela SIM.
* După finisarea cu succes a operației, semnătura digitală se expediază la Banca. Semnătura se păstrează ăn baza de date împreună cu pachetul original.
* După semnarea documentelor de către toate semnăturile necesare, documentului i se atribuie starea “Pentru banca”.

Documentele ce se află în starea “Pentru banca” odată pe minut se descarcă în SAB prin intermediul unui serviciu web intern special.

Documentele semnate pentru ziua curenta pot fi vizualizate in mapa “Semnate”.

Ulterior, documentele sunt transmise din Sistema DCD în SAB .

**9. Restabilirea Loghin-ului şi/sau Parolei**

Restabilirea Loghin-ului şi/sau Parolei poate fi efectuată prin contactarea Serviciul suport la numărul

de tel. 022 **57 67 69.** Parola se deblochează în baza identificării solicitantului, ca urmare a conversației cu operatorul parola se blochează sau poate fi deblocată; sau o nouă parolă poate fi trimisă la E-mail-ul specificat în contract.

**10. Securitatea Sistemului**

Securitatea Sistemului este asigurată prin:

* Sistemul utilizează software original aflat pe serverele Băncii.
* Schimbul de informație între dispozitivul clientului şi bancă se efectuează prin canale criptate (TLS/SSL);
* La nivelul serverului de aplicaţie e-Banking se utilizează un certificat SSL, achiziţionat de la compania ”DigiCert Inc”, care asigură autenticitatea serverului.
* Procesul de identificare a clientului se execută prin loghin-ul şi parola unică;.
* Pentru confirmarea documentelor ce urmează a fi achitate se folosește Semnătura Mobilă.

Dacă se pierde controlul asupra dispozitivului, clientul trebuie să informeze imediat serviciul suport la numărul

de tel. 022 **57 67 69** și filiala la care se deservește.

**11. Recomandări de utilizare securizată a Sistemului „Mobile Business”**

Urmatoarele recomandari sunt relatate in contract, pentru a minimiza riscurile legate de securitatea accesarii aplicatiei

* Să nu divulge informaţia confidenţială altor persoane terţe

(parole, conturi, datele personale);

* Să nu lase dispozitivul fără supraveghere, în special după procedura de autentificare şi să asigure că ecranul dispozitivului nu este vizibil altor persoane;
* Să seteze parola de acces la dispozitivul mobil şi opţiunea de blocare a dispozitivului după o perioadă de inactivitate;
* Să utilizeze parole şi coduri de acces puternice, pentru a evita spargerea lor;
* Să utilizeze diferite parole pentru fiecare serviciu (poşta electronică, conturile de acces la reţelele de socializare, etc.);
* Să descarce aplicaţiile mobile numai din magazinele oficiale AppStore, GooglePlay şi MarketPlace. Toate alte surse nu sunt oficiale şi Banca nu poartă răspundere pentru consecinţele instalării aplicaţiilor descărcate din aceste surse;
* Să efectueze regulat actualizarea sistemului de operare, aplicaţiei Mobile Business şi altor aplicaţii instalate pe dispozitivul mobil, utilizînd numai surse oficiale;
* Pentru a fi siguri că nu descărcaţi ceva dubios, dezactivaţi în setările telefonului pe platforma Android opţiunea „Surse Necunoscute” în setările de „Securitate”;
* Să instaleze pe dispozitivul mobil aplicaţii anti-virus şi să le actualizeze regulat. De asemenea trebuie actualizată aplicaţia anti-virus la calculatoarele la care se conectează dispozitivul mobil;
* Să nu păstreze pe dispozitivul mobil informaţie confidenţială;
* Aplicaţia Mobile Business va fi utilizată numai de Abonatul la Sistem;
* Să şteargă informaţia confidenţială în cazul transmiterii dispozitivului altor persoane (vinderea, reparaţia). Pentru aceasta este necesar să restabilească setările prestabilite din fabrică. Ştergerea informaţiei cu utilizarea punctelor de meniu va permite infractorului restabilirea ei;
* Să activeze opţiunea de control la distanţă pentru ştergerea datelor la distanţă sau blocare în cazul pierderii dispozitivului;
* Să nu execute operaţiunea de obţinere a dreptului de administrator (jail-break, rooting). Aceste operaţiuni pot scădea nivelul de securitate şi expune Sistemul unor riscuri suplimentare;
* În cazul pierderii sau furtului dispozitivului mobil, să schimbe urgent parola de acces la sistemul de deservire bancară la distanţă, să informeze imediat Banca pentru blocarea accesului la Sistem. Apoi să sune operatorul telefoniei mobile pentru blocarea cartelei SIM;

În cazul schimbării numărului de telefon sau neutilizării acestuia pentru o perioadă de timp mai mare decît valabilitatea cartelei SIM, să se adreseze Băncii pentru deconectarea Sistemului de la numărul de telefon pentru a evita compromiterea modalităţii de Autentificare Suplimentară;

* Să fie vigilenţi la atacurile de tip phişhing scopul cărora este obţinerea de la client a informaţiei confidenţiale. Să nu execute mesajele primite prin email sau SMS prin care se solicită divulgarea datelor confidenţiale. Banca niciodată nu transmite mesaje SMS şi email-uri pentru a solicita de la clienţi informaţie confidenţială;
* Să monitorizeze regulat operaţiunile executate;
* În cazul nefuncţionării cartelei SIM să sune imediat la operatorul telefoniei mobile pentru a se asigura că cauza nu este drept urmare a acţiunilor frauduloase;
* Să termine lucrul cu aplicaţia mobilă prin accesarea butonului Exit (Ieşire);
* Să ignoreze propunerile de instalare a unor „aplicaţii importante” sau „update-uri importante” dacă ele sunt primite de la persoane sau companii necunoscute (de exemplu prin email-uri, SMS, etc.);
* Să evite utilizarea reţelelor wireless/Wi-Fi publice (ex. in magazin, aeroport, pe strada, in cafenea, etc.) pentru operaţiuni bancare. Aceste puncte de acces pot fi controlate de infractori şi exista riscul ca datele transmise să fie compromise. Străduiţi-vă să utilizaţi numai reţele Wi-Fi securizate în care aveţi încredere. Se recomandă să dezactivaţi opţiunea de conectare automată la Wi-Fi

**12. Serviciile financiare ale Sistemului**

Tarifele referitoare la utilizarea *Serviciile financiare ale Sistemului*, sunt stabilite în *Tarifele BC „Moldindconbank” S.A.*