CURSUL Nr.7

SERVICII BANCARE ELECTRONICE

Introducere

Dezvoltarea si utilizarea “e-money” (monedei electronice) si a unor forme de “e-banking” (servicii bancare electronice) sunt încă într-o fază incipientă. Luând în considerare gradul ridicat de incertitudine al viitorului tehnologic şi al dezvoltării pieţelor pentru banca electronică şi pentru bani electronici, autorităţile care supraveghează aceste activităţi au recunoscut faptul că pe lângă beneficiile pe care le aduc aceste activităţi, există şi multe riscuri pentru bănci. De aceea, autorităţile care supraveghează activităţile “e” (electronice), precum şi băncile trebuie să dezvolte metode prin care să se identifice, administreze şi controleze riscurile asociate activităţilor de banca electronică şi bani electronici.

Dar, pentru a analiza riscurile care decurg din aceste activităţi trebuie mai întâi să le definim.

Definirea conceptelor

Comitetul de Supraveghere Bancară cu sediul la Basle defineşte ***activitatea de bancă electronică*** ca fiind activitatea de distribuire a serviciilor şi produselor bancare detailiste de valori diferite prin intermediul canalelor electronice.

Aceste produse şi servicii bancare pot include:

- atragerea depozitelor bancare,
- acordarea împrumuturilor,
- managementul contabil,
- acordarea de consultanţă financiară, precum şi
- furnizarea altor servicii şi produse de plată electronică cum ar fi moneda electronica.

Conceptului de ***bancă electronică/virtuală*** definită de revistele de specialitate ca fiind “banca în care contactul poate fi făcut printr-o varietate de canale, dar menţinând aceeaşi interfaţă şi accesând aceleaşi servicii”.

În mod obişnuit, cele mai la îndemână ***procedee prin care se distribuie consumatorilor produse şi servicii bancare electronice*** sunt:

- terminal POS (point of sale terminals),
- ATM-uri (automatic teller machine),
- telefoane mobile,
- calculatoare personale,

- terminal la distanţă,
- Video Kiosk,
- Internet şi altele.

Prin intermediul Internet-ului, o persoană poate avea acces 24 de ore/7 zile pe săptămână la conturile sale şi poate realiza tranzacţii, fiindu-i necesar pentru aceasta doar un calculator conectat la Internet şi un browser. Serviciile bancare prin Internet pot fi accesate şi prin dispozitivele mobile şi cu ajutorul WAP. Astfel, datorită extinderii sale rapide, Internet-ul aduce noi oportunităţi pentru industria bancară.

Din punctul de vedere al băncilor, ***segmentele de clienţi*** cărora li se adresează aceste servicii sunt:

- ***piaţa clienţilor individuali*** (se estimează că până la sfârşitul anului 2003 vor exista în SUA în jur de 18,5 milioane de utilizatori casnici);
- ***piaţa clienţilor instituţionali*** (clienţii corporaţionali).

Utilizarea Internet-ului pentru furnizarea produselor şi serviciilor bancare are avantaje pentru bănci şi pentru clienţi, aşa cum reiese din tabelul de mai jos:

Banca	➢ imagine bună pe piaţă; ➢ costuri reduse ale tranzacţiilor; ➢ răspuns rapid la cerinţele pieţei; ➢ creşterea veniturilor; ➢ creşterea numărului de clienţi.
Client individual	➢ costuri reduse pentru accesul şi folosirea diferitelor produse; ➢ comoditate; ➢ viteză; ➢ administrarea fondurilor;
Client instituţional	➢ costuri reduse ptr. accesarea şi utilizarea produselor; ➢ administrarea lichidităţilor.

Moneda electronica reprezintă banii depozitaţi prin mijloace electronice în vederea efectuării unor plăţi via terminal POS, transferuri directe, sau prin reţeaua calculatoarelor, aşa cum este Internet-ul.

Produsul cu valoare înmagazinată include:

- "hardware" sau mecanisme care se bazează pe cartele (numite "portofele electronice");
- "software" sau mecanisme care se bazează pe reţea (numite "digital cash").

Cartelele cu valoare înmagazinată pot să aibă: "o singură destinaţie" ("single-purpose"), aşa cum este cartela telefonică, şi pot fi utilizate pentru cumpărarea unui singur tip de marfă sau serviciu de

la un singur vânzător; cartele cu “mai multe destinaţii”(“multi-purpose”) care pot fi utilizate pentru mai multe cumpărări de la mai mulţi vânzători.

Băncile pot participa în circuitul monedei electronice:

- în calitate de emitenţi,
- dar pot îndeplini şi alte funcţii cum ar fi: distribuirea monedei electronice emise de alte entităţi, procesarea şi decontarea tranzacţiilor efectuate cu ajutorul monedei electronice,
- precum şi înregistrarea în contabilitate a tranzacţiilor respective.

Moneda electronica îmbracă mai multe forme*:*

1. ***“Debit cards***” – prin utilizarea acestora, consumatorul este împuternicit să cumpere mărfuri prin efectuarea unui transfer electronic al fondurilor direct din conturile lor personale de la bancă în conturile comerciantului.
2. ***“Stored-Value Card”*** – sunt carduri care se aseamănă cu cardurile de debit şi de credit, dar se disting prin faptul că ele conţin o sumă fixă de “digital cash”. Un tip sofisticat de stored-value card îl reprezintă cardul inteligent (“smart card”).
3. ***“Electronic cash”(“numerar electronic”)*** reprezintă un exemplu din lumea reală a sistemelor electronice de plăți, care folosesc poşta electronică sau Web-ul. “Numerarul electronic” se utilizează pe Internet pentru cumpărarea de bunuri şi servicii. Un consumator poate obţine “numerar electronic” prin deschiderea unui cont la o bancă care este racordată la Internet. Apoi, “numerarul electronic” este transferat pe calculatorul lui. Atunci când un client doreşte să cumpere o marfă cu “numerar electronic”, atunci el navighează pe Internet, caută un magazin şi selectează opţiunea de cumpărare a unui anumit articol, după care “numerarul electronic” este transferat automat de pe calculatorul clientului pe cel al comerciantului.
4. ***“Electronic Checks” (***“cecuri electronice”) – acestea permit utilizatorilor Internet-ului să-şi achite facturile direct prin Internet fără să mai transmită fila de cec. Utilizatorul calculatorului scrie valoarea echivalentă a cecului, după care transmite cecul electronic celeilalte părţi care la rândul ei îl transmite băncii sale.

Identificarea şi analizarea riscurilor

Datorită schimbărilor rapide intervenite în tehnologia informatică, băncile se confruntă cu riscuri specifice activităţilor de bancă electronică şi moneda electronica, riscuri prezentate în anexă. La acest nivel, ***se pare că riscul operaţional, riscul reputaţional şi riscul juridic reprezintă cele mai importante categorii de riscuri, în special pentru băncile internaţionale.***

- ***Riscul operaţional*** apare dintr-o potenţială pierdere datorată unor deficienţe semnificative în integritatea şi viabilitatea sistemului. Considerentele de securitate sunt supreme, dacă băncile sunt subiecte de atac extern sau intern asupra produselor şi sistemelor lor. Riscul operaţional

poate apărea din neutilizarea corectă a sistemelor de bani electronici sau bancă electronică, precum şi din realizarea sau implementarea neadecvată a acestor sisteme. În această categorie se încadrează următoarele riscuri:

- ***Riscul de securitate***. Controlarea accesului la sistemele băncii a devenit din ce în ce mai complexă datorită capacităţilor dezvoltate ale calculatorului, dispersării geografice a punctelor de acces şi utilizării variatelor căi de comunicaţii incluzând reţelele publice cum ar fi Internet-ul. Accesul neautorizat la reţea ar putea conduce la pierderi directe, adăugarea unor datorii clienţilor, etc. Ar putea, de asemenea, avea loc o varietate a problemelor de autentificare şi acces specific. De exemplu, controalele neadecvate ar putea conduce la atacuri reuşite ale hacker-ilor care operează prin Internet, care ar putea accesa, salva şi utiliza informaţii confidenţiale despre clienţi. În lipsa unor controale adecvate, o terţă persoană ar putea avea acces la sistemul computerizat al băncii şi ar putea să-l viruseze. Pe lângă atacurile externe asupra sistemelor băncii electronice şi banilor electronici, băncile sunt expuse riscului operaţional în ceea ce privește frauda angajaţilor. Angajaţii ar putea achiziţiona clandestin date legate de autentificare în vederea accesării conturilor clienţilor sau pentru furarea cardurilor cu valoare înmagazinată. Erorile datorate angajaţilor ar putea, de asemenea, compromite sistemele băncii. O importanţă deosebită pentru autorităţile de supraveghere o prezintă riscul contrafacerii banilor electronici, faptă care potrivit codului penal reprezintă infracţiuni. Acest risc poate fi mărit dacă băncile eşuează în incorporarea măsurilor adecvate pentru descoperirea şi împiedicarea contrafacerilor. O bancă se confruntă cu riscul operaţional din falsificări şi devine datoare cu suma soldului banilor electronici falsificaţi. Mai pot apărea, de asemenea, şi costuri datorate reparaţiilor unui sistem compromis.
- ***Riscuri legate de proiectarea, implementarea şi întreţinerea sistemelor***. Astfel, o bancă este expusă riscului unei întreruperi sau încetiniri a sistemelor sale, dacă banca electronică sau banii electronici aleşi de bancă nu sunt compatibile cu cerinţele utilizatorului.
- ***Riscuri care apar datorită folosirii necorespunzătoare de către clienţi a produselor şi serviciilor bancare***. Riscul este mărit atunci când o bancă nu îşi educă corespunzător clienţii cu privire la precauţiile de securitate. În plus, în lipsa existenţei unor măsuri adecvate de verificare a tranzacţiilor, clienţii ar putea să respingă tranzacţiile pe care le-au autorizat în trecut, creându-i astfel băncii numeroase pierderi financiare. Clienţii care folosesc informaţii personale (informaţii de autentificare, numere de cărţi de credit etc.) într-o transmitere electronică neasigurată poate permite persoanelor rău intenţionate să obţină accesul la conturile clienţilor. Ca urmare, banca poate suferi pierderi financiare din cauza tranzacţiilor neautorizate. Spălarea banilor poate fi o altă sursă de îngrijorare.

- ***Riscul reputaţional*** este riscul datorat unei opinii publice negative semnificative care constă într-o piedere critică a fondurilor sau clienţilor băncii. Riscul reputaţional poate apărea atunci când acţiunile băncii produc o piedere majoră a încrederii publicului în abilitatea băncii de a îndeplini funcţii critice pentru a-şi continua activitatea. Riscul reputaţional este important nu numai pentru o singură bancă, ci acesta este important pentru întreg sistemul bancar.
- ***Riscul juridic*** apare prin violarea sau neconformarea cu legile, regulile, reglementările sau practicile prescrise, sau atunci când drepturile şi obligaţiile legale ale părţilor participante la o tranzacţie nu sunt stabilite corect. Băncile angajate în activităţile de "e-banking" sau "e-money" se pot confrunta cu riscuri juridice referitoare la dezvăluirea unor informaţii privind clienţii şi la protecţia secretului bancar.
- ***Alte riscuri*** Riscurile bancare tradiţionale cum sunt riscul de credit, riscul de lichiditate, riscul ratei dobânzii şi riscul de piaţă sunt riscuri care pot apărea şi în activitatea băncii electronice. ***Riscul de credit*** reprezintă riscul care apare datorită neachitării în întregime a unei obligaţii de plată, fie la termenul stabilit sau în orice moment stabilit după aceea. Băncile care desfăşoară activitatea de bancă electronică pot să-şi extindă creditul prin canale netradiţionale şi să-şi extindă piaţa dincolo de graniţele geografice tradiţionale. Procedurile neadecvate prin care se determină credibilitatea debitorilor care solicită credite prin canale electronice pot determina riscurile de credit pentru băncile respective. ***Riscul de lichiditate*** reprezintă riscul care apare datorită incapacităţii băncii de a-şi îndeplini obligaţiile atunci când vin scadenţele. ***Riscul ratei dobânzii*** se referă la expunerea situaţiei financiare a băncii la mişcările nedorite ale ratelor dobânzii. ***Riscul de piaţă*** este riscul piederilor înregistrate în poziţiile din interiorul bilanţului, cât şi în cele din afara acestuia, pierderi care apar datorită mişcărilor preţurilor de piaţă, incluzându-se şi cursurile de schimb valutar.
- ***Riscul de management*** Un proces de administrare al riscurilor care include cele trei elemente de bază evaluarea riscului, controlul expunerii la risc şi monitorizarea riscurilor va ajuta băncile şi supraveghetorii să atingă aceste obiective. Este esenţial ca băncile să aibă o gestionare transparentă a riscurilor. Iar atunci când sunt identificate noi riscuri în aceste activităţi, consiliul de administraţie şi conducerea executivă trebuie informate.

Stabilirea riscurilor

Stabilirea riscurilor este un proces continuu, care presupune realizarea următoarelor trei etape:

- ***Banca se angajează într-un proces analitic de identificare a*** riscurilor şi acolo unde este posibil, de comensurare a acestora. În cazul în care riscurile nu pot fi comensurate, conducerea băncii stabileşte riscurile potenţiale care pot apărea, paşii de urmat şi stabileşte impactul pe care îl poate avea asupra băncii.

- Stabilirea riscului înseamnă pentru bancă ***determinarea toleranţei de risc a băncii, lucru care înseamnă stabilirea pierderilor pe care şi le permite banca în cazul apariţiei unor evenimente neprevăzute.***
- ***Conducerea băncii poate compara toleranţa riscului cu magnitudinea stabilită pentru un anumit risc, pentru a se stabili dacă riscul respectiv se înscrie în limitele toleranţei***.

Gestionarea şi controlul riscurilor

După stabilirea riscurilor şi a toleranţelor acestora, conducerea băncii trebuie să le gestioneze şi să le controleze. ***Această etapă a gestionării riscului include*** activităţi ca:

- ***coodonarea comunicării interne***,
- ***implementarea măsurilor de protecţie*** împotriva riscurilor din exterior,
- ***controlul şi gestionarea*** lor,
- ***instructarea clienţilor în utilizarea serviciilor*** etc.

Băncile îşi măresc abilitatea în controlul şi gestionarea riscurilor inerente în orice activitate atunci când toate acestea sunt stabilite prin proceduri şi sunt la îndemâna întregului personal.

Procesul de gestionare şi control al riscurilor include:

- ***Politici şi măsuri de securitate***. Securitatea reprezintă o combinaţie de sisteme, aplicaţii practice şi control intern utilizate pentru a pune la adăpost integritatea, autenticitatea şi confidenţialitatea datelor şi procedeelor de operare. Politica de securitate enunţă intenţiile managementului firmei de a susţine securitatea informaţiilor, dă o explicaţie cu privire la organizarea securităţii unei bănci, precizează direcţiile principale care definesc toleranţa riscului de securitate al unei bănci. Politica conturează responsabilităţile pentru modelarea, implementarea şi întărirea măsurilor de securitate a informaţiei, ea mai poate stabili procedurile pentru evaluarea rezultatelor politicii, pentru întărirea măsurilor disciplinare şi pentru raportarea violării securităţii. Măsurile de securitate include: criptarea, parolarea, depistarea viruşilor etc.
- ***Comunicarea internă***. Conducerea (management superior) trebuie să comunice personalului cheie cum prevederile sistemelor de bancă electronică şi bani elecronici intenţionează să susţină scopurile generale ale băncii. În acelaşi timp, personalul tehnic trebuie să comunice clar conducerii cum sunt proiectate sistemele să funcţioneze, care sunt punctele tari şi slabe ale sistemului. Pentru asigurarea unei comunicări interne adecvate, toate procedurile trebuie prevăzute în scris. În scopul limitării riscului operaţional, conducerea trebuie să adopte o politică comună de educare continuă a cunoştinţelor personalului cu noutăţile tehnologice.

- ***Evaluarea produselor şi serviciilor înainte ca ele să fie introduse pe o scară largă*** poate limita riscurile operaţionale şi de reputaţie.Testarea validează faptul că echipamentul şi sistemele funcţionează şi produc rezultatele dorite. Programele pilot sau prototipurile pot fi de asemenea de ajutor în dezvoltarea unor aplicaţii informatice noi.

În vederea reducerii riscurilor enumerate este necesară reglementarea tuturor activităţilor "e", stabilirea unei infrastructuri adecvate, precum şi precizarea celor care trebuie să autorizeze şi supravegheze aceste activităţi.

Ca orice operaţiune comercială, ***comerţul electronic are nevoie de o infrastructură specifică.*** În acest caz, ***aceasta se compune din trei elemente***: infrastructura tehnică, interfaţa cu componentele comerciale clasice şi sistemul juridic specific.

- ***Infrastructura tehnică*** este constituită din sistemele hardware, softwarw-ul aferent şi reţeaua de comunicaţii. Aceasta constituie de fapt şi componenta care a determinat apariţia şi dezvoltarea comerţului electronic.
- Este, de asemenea, necesară o ***interfaţă majoră cu sistemele clasice de comerţ.*** Elementul cheie îl reprezintă banca, întrucât orice operaţiune comercială este mijlocită de bani. Inserarea unei bănci în sistemul de comerţ electronic presupune o conexiune securizată între bancă şi utilizator prin intermediul căreia să se poată efectua operaţiunile în timp real.
- În vederea ***creării cadrului legal pentru*** ţările membre ale Comunităţii Europene, Parlamentul European a adoptat Directivele nr. 1999/93/EC din 13 decembrie 1999 cu privire la crearea cadrului legal pentru semnătura electronică, precum şi nr. 2000/31/EC din 8 iunie 2000 cu privire la comerţul electronic.

Semnătura electronică reprezintă o informaţie ataşată unui document electronic care identifică în mod unic semnatarul, fiind realizată cu mijloace aflate exclusiv în posesia acestuia, ea identificând documentul şi semnalând orice modificare ulterioară adusă acestuia.

Băncile româneşti (cele afiliate la Romcard: Banca Comercială Română SA, Banca Română pentru Dezvoltare SA, Banca Agricolă SA, Banca Comercială Ion Tiriac SA) au lansat produse din categoria cardurilor, Raiffeisen Bank SA şi băncile olandeze au lansat "multi cash-ul", un fel de home banking services, iar Banca Turco-Română SA a lansat serviciul de Internet-banking.

Concluzii

Având în vedere avantajele banilor electronici şi a serviciilor bancare electronice, s-a afirmat că economia se va îndrepta cu paşi repezi spre o societate baza pe lipsa fizică a numerarului, societate în care toate plăţile se vor efectua electronic. Deşi, s-a prezis încă din anii 1975 că lumea se va baza

foarte curând pe o astfel de societate, totuşi mişcarea către o societate lipsită de numerar se realizează foarte greu.

Deşi, mijloacele electronice de plată pot fi mult mai eficiente decât un sistem de plăţi bazat pe hârtie, mai mulţi factori luptă împotriva dispariţiei sistemului bazat pe hârtie şi în România, datorită următoarelor:

1. economia României nu este pregătită pentru un astfel de sistem, neexistând cultura economică necesară intrării în joc;
2. neexistenţa legislaţiei în domeniu (reglementări privind criptarea, privind efectuarea plăţilor prin Internet, precum şi privind efectuarea plăţilor cu ajutorul numerarului electronic);
3. neexistenţa sistemelor digitale de plăţi ajunse la o utilizare de masă;
4. inerţia sistemului actual;
5. costurile mari cu întreţinerea hardului şi softului utilizat;
6. neîncrederea în sistemului electronic.

In Romania, domeniul serviciilor bancare electronice si al platilor prin carduri este reglementat de Banca Nationala a Romaniei care a emis, in acest sens, Regulamentul nr.6/13.06.2006 privind emiterea şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente şi precizările BNR referitoare la aplicabilitatea acestuia. Regulament se aplica bancilor, persoane juridice romane, precum si sucursalelor din Romania ale bancilor, persoane juridice straine si are ca obiect stabilirea principiilor privind emiterea si utilizarea instrumentelor de plata electronica pe teritoriul Romaniei, in special a cardurilor si a conditiilor care trebuie indeplinite de catre banci si alti participanti la desfasurarea activitatii de plati cu instrumente de plata electronica, indiferent de moneda in care sunt emise/denominate acestea.

In conformitate cu prevederile regulamentului amintit, bancile vor pune in circulatie numai instrumente de plata electronica autorizate, in prealabil, de catre Banca Nationala a Romaniei.

In vederea obtinerii autorizatiei pentru emiterea instrumentelor de plata electronica, solicitantul trebuie sa prezente Bancii Nationale a Romaniei – Directia Reglementare si Autorizare urmatoarele documente:

a) cererea de autorizare insotita de 2 specimene ale instrumentului de plata electronica care se doreste a fi emis;

b) normele si procedurile interne legate de instrumentele de plata electronica, aprobate de consiliul de administratie al solicitantului;

c) in cazul in care solicitantul nu este proprietar de marca, se vor anexa la cererea de autorizare toate certificarile si aprobarile primite de la proprietarul de marca cu privire la designul si conditiile tehnice de executare a cardului, a hardware-ului si a software-ului utilizat;

d) in situatia in care cardurile sunt cu circulatie internationala, iar solicitantul nu este proprietar de marca, se vor anexa si certificarile proprietarului de marca cu privire la integrarea in sistemul de autorizare a tranzactiilor si cel de decontare a acestora;

e) in situatia in care se solicita autorizarea pentru un sistem bazat pe un instrument de plata electronica de tipul chip-card, domestic card si/sau card cu circulatie internationala, cererea va fi insotita de o scrisoare de certificare din partea VISA International S.A. sau Europay International S.A. din care sa rezulte ca instrumentul de plata electronica este compatibil cu specificatiile EMV (Europay/Mastercard/VISA), ultima editie, valabila la data cererii; certificarea nu este necesara in cazul in care chip-ul inglobat in instrumentul de plata este folosit in alte scopuri decat cele de plati (identificare, acces etc.);

f)]n situatia in care emitentul solicita autorizarea pentru un instrument de plata cu acces la distanta, de tipul aplicatiilor Internet-banking sau home-banking, cererea va fi insotita de toate avizele/certificarile primite de la producatorul programului informatic – software-ului aflat la baza aplicatiei -, privind nivelul de securitate al transmisiilor de date si protocolul de raspuns utilizat in cazul aparitiei unor disfunctionalitati in cadrul sistemului, precum si de avizul Ministerului Comunicatiilor si Tehnologiei Informatiilor sau al altor entitati indicate de acesta;

g) un business plan care va cuprinde, fara a se limita la, urmatoarele elemente:

g_1) Informatii privitoare la emitent:

- numarul si tipul conturilor si al sediilor secundare (sucursale, agentii);
- alte instrumente de plata emise si autorizate de Banca Nationala a Romaniei pâna la momentul prezentarii cererii de autorizare;
- descrierea detaliata a sistemului informatic al emitentului, utilizat pentru desfasurarea activitatilor legate de emiterea unui instrument de plata electronica.

g_2) Informatii despre instrumentul de plata electronica:

- tipul instrumentului de plata electronica ce urmeaza a fi emis;
- serviciile ce urmeaza a fi oferite prin intermediul instrumentului de plata electronica;
- moneda in care este denominat instrumentul de plata electronica;
- modalitatile de identificare, urmarire si gestionare a riscurilor ce pot fi induse de utilizarea frauduloasa a instrumentului de plata electronica.

g_3) Informatii despre aria de utilizare a instrumentului de plata electronica:

- numarul de clienti potentiali ;
- zona geografica de utilizare (card cu circulatie interna sau card cu circulatie internationala);

g_4) Obiective:

- numarul instrumentelor de plata electronica care vor fi emise;

- modul de efectuare a analizei de solvabilitate in cazul cardurilor de credit;
- estimarea numarului anual de tranzactii;
- data la care se intentioneaza inceperea emiterii instrumentului respectiv;
- canalele de distributie (la ghiseu, sucursale, prin posta etc.);
- tipul de hardware si software ce urmeaza a fi folosit;
- strategia de promovare a produsului, modul de organizare a campaniei publicitare;
- estimare pe durata a 3 ani a veniturilor si cheltuielilor legate de instrumentul de plata electronica si utilizarea acestuia.

Dupa analizarea documentatiei prezentate, in cazul in care decizia este favorabila, Banca Nationala a Romaniei va emite solicitantului o *autorizatie provizorie*, valabila 90 zile, perioada in care solicitantul se va afla sub monitorizarea speciala a Bancii Nationale a Romaniei.

Principalele obiective urmarite in perioada de monitorizare sunt:

a) derularea zilnica a operatiunilor;
b) analizarea saptamanala a statisticilor rezultate din utilizarea instrumentelor de plata electronica, in scopul prevenirii unor potentiale probleme;
c) analizarea desfasurarii activitatii serviciului de gestiune a riscului (daca exista);
d) analizarea modului de decontare a operatiunilor;
e) elaborarea de rapoarte saptamanale de monitorizare.

In situatia in care rezultatele obtinute in perioada de monitorizare indeplinesc conditiile prevazute regulamentul amintit, Banca Nationala a Romaniei va emite solicitantului autorizatia definitiva pentru tipul de instrument de plata electronica precizat in cererea de autorizare.

Calitatea de detinator se acorda de catre emitent, potrivit regulamentului, emitentul asumându-si obligatia sa verifice cel putin urmatoarele date:

a) identitatea solicitantului;
b) autenticitatea documentelor prezentate;
c) veridicitatea si actualitatea informatiei;
d) orice date si elemente pe care emitentul le-ar putea considera necesare pentru evaluarea activitatii si faptelor clientului care ar putea genera riscuri la plata cu instrumentul de plata electronica;

La emiterea unui card sub licenta unui proprietar de marca, emitentul executa mandatul acestuia in termenele si conditiile contractului incheiat cu acesta.

Pe baza cererii aprobate de emitent, acesta va incheia si semna un contract cu detinatorul, contract ce va cuprinde prevederi exprese privind drepturile si obligatiile partilor.

Dupa incheierea contractului, reprezentantul autorizat al emitentului va elibera detinatorului un card personalizat impreuna cu plicul special care contine PIN-ul (Numarul de Identificare al Persoane) sau codul care permite identificarea detinatorului/utilizatorului si accesul la contul detinatorului de card.

Trebuie mentionat, de asemenea ca, in conformitate cu reglementarile valutare in vigoare, decontarea operatiunilor efectuate cu carduri pe teritoriul Romaniei, indiferent de moneda in care sunt emise/denominate acestea, se va efectua numai in moneda nationala.