

ORDIN

privind procedura de avizare a instrumentelor de plată cu acces la distanță, de tipul aplicațiilor internet-banking, home-banking sau mobile-banking

CAPITOLUL I: Dispoziții generale

Art. 1

Prezentul ordin se aplică băncilor, persoane juridice române, precum și sucursalelor din România ale băncilor, persoane juridice străine, denumite în continuare bănci, și are ca obiect stabilirea procedurii privind eliberarea avizului Ministerului Comunicațiilor și Societății Informaționale asupra instrumentelor de plată cu acces la distanță tip internet-banking, home-banking sau mobile-banking.

Art. 2

În înțelesul prezentului ordin, termenii și expresiile de mai jos au următoarele semnificații:

- a)** instrument de plată cu acces la distanță - soluția informatică ce permite utilizatorului să aibă acces la distanță la fondurile aflate în contul deținătorului, și prin intermediul căruia se pot efectua plăți către un beneficiar sau alt gen de operațiuni de transfer de fonduri și care necesită, de regulă, un nume de utilizator ori un cod personal de identificare/parolă sau orice altă dovadă a identității, necesară autentificării. Instrumentul de plată cu acces la distanță mai poate furniza posibilitatea transmiterii electronice a instrucțiunilor de plată din contul propriu și a transcrierii mesajului dorit pe ordinul de plată care va fi generat automat de sistem, utilizatorul poate efectua și operațiuni de schimb valutar, poate constitui depozite și poate obține informații privind soldul conturilor și al operațiunilor efectuate.
- b)** emitent - banca autorizată de Banca Națională a României să emită instrumente de plată electronică și care pune la dispoziție deținătorului un instrument de plată electronică cu acces la distanță, pe baza unui contract încheiat cu acesta;
- c)** deținător - persoana fizică sau juridică care, în baza contractului încheiat cu emitentul, deține un mecanism de autentificare în utilizarea instrumentului de plată cu acces la distanță;
- d)** utilizator - deținătorul instrumentului de plată cu acces la distanță sau o persoană fizică recunoscută și acceptată de către deținător ca având acces la drepturile sale conferite de către emitent;
- e)** instrument de plată cu acces la distanță tip Internet-banking - acel instrument de plată cu acces la distanță care se bazează pe tehnologia Internet (world wide web) și pe sistemele informatice ale emitentului;
- f)** instrument de plată cu acces la distanță tip home-banking - acel instrument de plată cu acces la distanță care se bazează pe o aplicație software a emitentului instalată la sediul deținătorului pe o stație de lucru individuală sau în rețea;
- g)** instrument de plată cu acces la distanță tip mobile-banking - acel instrument de plată cu acces la distanță care presupune utilizarea exclusivă a unui echipament mobil (telefon, PDA - Personal Digital Assistant etc.) și a unor servicii oferite de către operatorii de telecomunicații;
- h)** plan de securitate - documentul ce descrie totalitatea măsurilor tehnice și administrative care sunt luate de către emitent pentru utilizarea în condiții de siguranță a instrumentului de plată cu acces la distanță;
- i)** aviz - actul administrativ emis de Ministerul Comunicațiilor și Societății Informaționale în conformitate cu prevederile art. 30, alin. B, lit. d) din Regulamentul Băncii Naționale a României nr. 6/2006 privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, care conferă solicitantului dreptul de a obține autorizația din partea Băncii Naționale a României pentru emiterea instrumentului de plată cu acces la distanță;
- j)** BNR - Banca Națională a României;

- k)** Regulamentul nr. 6 al BNR - Regulamentul Băncii Naționale a României nr. 6/2006 privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, publicat în Monitorul Oficial al României, Partea I, nr. 927 din 15 noiembrie 2006;
- l)** MCSI - Ministerul Comunicațiilor și Societății Informaționale;
- m)** CISA - Certified Information Systems Auditor (auditorul pentru sisteme informatice, certificat de ISACA);
- n)** ISACA - Information Systems Audit and Control Association.
- o)** test de penetrare – teste realizate cu permisiunea proprietarului unui sistem informatic care verifică securitatea rețelei și a aplicațiilor simulând atacuri din perspectiva unei persoane rău intenționate
- p)** LPT - Licensed Penetration Tester

Art. 3

Scopul avizului îl constituie verificarea îndeplinirii de către sistemul informatic al emitentului și de către soluția software, prin intermediul căreia este oferit instrumentul de plată cu acces la distanță, a unor cerințe minime de securitate, referitoare la:

- a)** confidențialitatea și integritatea comunicațiilor;
- b)** confidențialitatea și nonrepudierea tranzacțiilor;
- c)** confidențialitatea și integritatea datelor;
- d)** autenticitatea părților care participă la tranzacții;
- e)** protecția datelor cu caracter personal;
- f)** păstrarea secretului bancar;
- g)** trasabilitatea tranzacțiilor;
- h)** continuitatea serviciilor oferite clienților;
- i)** împiedicarea, detectarea și monitorizarea accesului neautorizat în sistem;
- j)** restaurarea informațiilor gestionate de sistem în cazul unor calamități naturale și evenimente imprevizibile;
- k)** gestionarea și administrarea sistemului informatic;
- l)** orice alte activități sau măsuri tehnice întreprinse pentru exploatarea în siguranță a sistemului.

Art. 4

Măsurile tehnice și organizatorice întreprinse pentru îndeplinirea cerințelor enumerate la art. 3 vor fi în concordanță cu progresul tehnologic și cu riscurile potențiale.

CAPITOLUL II: Eliberarea avizului

Art. 5

Documentele necesare pentru eliberarea avizului sunt:

- a)** cererea de eliberare a avizului, adresată în acest scop MCSI, conform modelului prevăzut în anexa nr. 1;
- b)** licența de funcționare a emitentului, acordată de BNR, sau notificarea transmisă de autoritatea competentă din statul membru de origine către BNR;
- c)** descrierea funcțională a sistemului informatic prin intermediul căruia este oferit instrumentul de plată cu acces la distanță;
- d)** planul de securitate al sistemului informatic, aprobat prin semnătură de către reprezentantul legal al emitentului, cuprinzând totalitatea măsurilor tehnice și organizatorice prevăzute pentru asigurarea cerințelor cuprinse la art. 3;
- e)** certificările din punctul de vedere al securității, asupra soluției informatice sau produselor conținute în aceasta, emise de organizații naționale sau internaționale recunoscute, acolo unde există;
- f)** opinia de audit asupra planului de securitate prevăzut la lit. d) și a soluției informatice prin intermediul căreia este oferit instrumentul de plată cu acces la distanță;
- g)** o declarație în care este exprimată independența auditorului față de sistemul informatic auditat prin intermediul căreia se certifică faptul că membrii echipei de audit și societățile comerciale la care sunt

angajați nu au fost impălicați în misiuni de consultanță legate de sistemul auditat. Declarația va fi semnată de către toți membrii echipei de audit și semnate și ștampilate de către reprezentantul legal al fiecărui angajator.

Art. 6

(1) Opinia de audit prevăzută la art. 5, pct. f), va fi întocmită de către o persoană certificată ca auditor de sisteme informatice (CISA emisă de către ISACA) și va fi semnată către auditorul șef, ștampilată și înregistrată. Opinia de audit va conține cel puțin următoarele informații:

- a) data emiterii
- b) componența echipei de audit și calificările acestora (care se vor anexa în copie)
- c) perioada auditului
- d) standardele folosite ca referință în timpul auditului
- e) modul în care s-a realizat auditarea pentru sistemele informatice situate în afara țării
- c) sumar al rezultatului auditului și al testelor de penetrare și specificarea eventualelor rezerve

(2) Misiunea de audit în baza căreia se emite opinia de audit poate fi efectuată de către o echipă cu următoarea componență minimală:

- a) un auditor șef certificat ca auditor de sisteme informatice (CISA emisă de către ISACA)
- b) un expert în teste de penetrare având certificarea Licensed Penetration Tester (LPT) emisă de către EC Council.

(3) Auditul efectuat va acoperi cel puțin următoarele domenii:

- a) Verificarea documentației de avizare
- b) Identificarea și evaluarea riscurilor potențiale
- c) Verificarea proceselor și fluxurilor de lucru ale sistemului
- d) Verificarea procedurilor de înregistrare administrator
- e) Verificarea procedurilor de înregistrare utilizatori
- f) Verificare proceselor de autentificare
- g) Verificarea securității bazelor de date
- h) Verificarea protecției sistemelor de operare, a routerelor, firewall-urilor și a switch-urilor
- i) Verificarea protecției antivirus
- j) Verificarea proceselor de backup, restaurare și dovezi ale testării procedurilor de restaurare
- k) Verificarea procedurilor administrative
- l) Scanarea porturilor și vulnerabilităților potențiale
- m) Verificarea proceselor de administrare ale sistemului
- n) Efectuarea de teste de penetrare asupra rețelei, a echipamentelor de rețea, a siturilor web și a bazelor de date, simulând atacuri reale atât din afara rețelei cât și din interior.
- o) Verificarea protejării datelor personale și datelor privind conturile bancare ale unui utilizator al sistemului și imposibilitatea de a fi accesate de către alți utilizatori neautorizați să o facă
- p) Simularea efectuării de tranzacții neautorizate prin vicierea mecanismelor de autentificare a utilizatorilor și de validare a tranzacțiilor
- q) Verificarea rezistenței la atacuri cunoscute precum: Cross-Site Scripting, Cross-Site Request Forgery, SQL Injection, XPATH Injection, LDAP Injection, Malicious File Execution, Insecure Direct Object Reference, Denial of Service, Remote File Inclusion
- r) Verificarea și testarea modului de criptare și stocare internă a datelor
- s) Vulnerabilități ale tehnologiilor folosite: Flash, Java, CGI, etc

(4) În procesul de auditare, auditorul poate solicita concursul altor experți. Auditorul poate echivala un test de penetrare efectuat în ultimele 6 luni.

(5) La cererea expresă a MCSI, precum și în cazul opiniilor de audit exprimate cu rezerve, emitentul va pune la dispoziție raportul de audit și raportul testelor de penetrare rezultate în urma auditării sistemului.

(6) Pentru cazurile în care sistemul informatic prin intermediul căruia este oferit instrumentul de plată cu acces la distanță este situat în afara țării, auditarea sistemului se va face prin una dintre următoarele metode:

- a) auditorul român va audita sistemele din străinătate; sau
- b) auditorul român agreează auditarea sistemului din străinătate de către personal cu calificare similară din acea țară și emite o opinie pe baza raportului auditorului strain; acest raport trebuie să fie emis cu cel mult șase luni înaintea depunerii documentației de avizare și trebuie să cuprindă rezultatul auditului de securitate al sistemului supus avizării, inclusiv testele de penetrare

Art. 7

Documentele prevăzute la art. 5 se vor transmite către MCSI, îndosariate/broșate și numerotate, în limba română.

Art. 8

Planul de securitate se va întocmi respectându-se următoarea structură:

1. Informații de identificare:

- a) emitentul instrumentului de plată cu acces la distanță;
- b) denumirea instrumentului de plată cu acces la distanță;
- c) producătorul instrumentului de plată cu acces la distanță;
- d) categoria (internet, home sau mobile-banking);
- e) statutul operațional al sistemului prin intermediul căruia este oferit instrumentul de plată cu acces la distanță și anul intrării în producție;
- f) descrierea generală a soluției tehnice;
- h) interconectarea sistemului cu sisteme interne sau externe;
- i) aria geografică în care instrumentul de plată cu acces la distanță poate fi utilizat;
- j) datele de contact ale persoanelor responsabile.

2. Senzitivitatea sistemului:

- a) legislația aplicabilă, care să cuprindă acele acte legislative și normative, reglementări și ultimile versiuni de standarde recunoscute și recomandate în domeniu sau care le înlocuiesc pe acestea, dintre cele detaliate în lista din anexa nr. 6, alte prevederi legale naționale cu efect/aplicabilitate asupra domeniului de interes, respectiv reglementările aplicate la nivel internațional și/sau în statul respectiv, pentru cazul în care sistemul informatic prin intermediul căruia este oferit instrumentul de plată cu acces la distanță este situat în afara țării.
- b) descrierea generală a sensibilității informațiilor gestionate de către sistem.

3. Măsurile pentru securitatea sistemului:

- a) evaluarea și managementul riscurilor potențiale;
- b) codurile de conduită/condițiile de utilizare/contractul prin care este oferit instrumentul de plată cu acces la distanță;
- c) rapoartele anuale de testare, care să conțină și rezultatele finale privind acceptanța modului de implementare și funcționare a procedurilor operaționale aprobate, respectiv funcționarea corectă a resurselor hardware și software din compunerea sistemului informatic destinat instrumentului de plată cu acces la distanță;
- d) măsurile tehnice de securitate implementate, în care să fie detaliate soluțiile și modalitățile de îndeplinire a cerințelor de securitate prevăzute la art. 3 din prezentul ordin;
- e) procedurile operaționale de exploatare;
- f) măsurile aplicate pentru asigurarea securității fizice;
- g) instruirea personalului propriu al emitentului în legătură cu administrarea sistemului informatic;
- h) instrucțiunile de utilizare a instrumentului de plată cu acces la distanță (manualul de utilizare oferit clienților);
- i) suportul tehnic oferit de către emitent clienților care utilizează instrumentul de plată cu acces la distanță.

4. Orice alte informații relevante legate de măsurile luate de către emitent pentru a asigura exploatarea în siguranță a instrumentului de plată cu acces la distanță.

Art. 9

- (1) Documentele prevăzute la art. 5 se înaintează către MCSI în perioada 1 aprilie - 30 noiembrie în anul 2009 și 1 aprilie – 30 iunie a fiecărui an începând cu anul 2010.
- (2) Avizul eliberat este valabil până la data de 1 iulie a anului următor.
- (3) Perioada de valabilitate a avizelor valabile la data emiterii prezentului ordin se prelungește din oficiu până la 1 decembrie 2009.
- (4) Avizul eliberat este netransmisibil.

Art. 10

În cazul emiterii unui nou instrument de plată cu acces la distanță după data de 1 iulie, emitentul poate solicita avizul MCSI odată cu depunerea documentelor necesare, prevăzute la art. 5.

Art. 11

- (1) În cazul în care, pe perioada de valabilitate a avizului, emitentul dezvoltă sau implementează noi module de aplicație sau platforme hardware/software, efectuează modificări de proceduri operaționale sau modifică măsurile tehnice de securitate aplicabile instrumentului de plată cu acces la distanță, acesta va notifica aceste modificări către MCSI.
- (2) Notificarea prevăzută la alin. (1) se va face în termen de 30 de zile de la data la care modificările specificate la alin. (1) devin operaționale.
- (3) În urma notificării, dacă se consideră că modificările efectuate afectează major securitatea sistemului informatic prin intermediul căruia este oferit instrumentul de plată cu acces la distanță, MCSI sau BNR pot solicita emitentului reinițierea procedurii de obținere a unui nou aviz, cu respectarea prevederilor art. 5-8 din prezentul ordin.
- (4) Dacă solicitarea prevăzută la alin. (3) este efectuată de MCSI, acesta va notifica în același timp și BNR.

Art. 12

- (1) Documentele enumerate la art. 5 vor fi întocmite și transmise la sediul MCSI într-un singur exemplar, iar acolo unde este cazul, vor fi clasificate din punctul de vedere al conținutului acestora, conform legislației în vigoare și procedurilor emitentului care solicită avizarea.
- (2) Al doilea exemplar al documentelor enumerate la art. 5 (mai puțin documentele solicitate la punctele f) și g) ale aceluiași articol, care pot fi inserate în copie, în cazul în care auditorul le-a întocmit numai în câte un singur exemplar) vor fi păstrate de către emitent la sediul acestuia, pe toată durata de valabilitate a avizului.

Art. 13

- (1) În situația prevăzută la art. 9, în urma analizării documentației prezentate, în termen de 20 de zile lucrătoare de la data înregistrării acesteia la MCSI, acesta va comunica solicitantului decizia sa cu privire la acordarea avizului și va notifica BNR în legătură cu aceasta.
- (2) Dacă la sediul MCSI se vor prezenta în aceeași zi lucrătoare mai mult de 5 emitenți pentru a înregistra documentațiile prevăzute la art. 5, atunci termenul estimat la alin. (1), începând cu a șasea documentație, se va mări cu câte un interval de timp cel puțin 1-3 zile lucrătoare pentru analizarea fiecărei documentații înregistrate în plus, iar MCSI va informa emitenții în cauză, inclusiv pe cei care vor sosi în zilele imediat următoare, despre mărirea termenului legal de comunicare cu privire la eliberarea avizului.
- (3) În situația prevăzută la art. 10, în urma analizării documentației prezentate, în termen de 15 zile de la data înregistrării acesteia la MCSI, acesta va comunica solicitantului decizia sa cu privire la acordarea avizului și va notifica BNR în legătură cu aceasta, conform modelului din anexa nr. 7.
- (4) După eliberarea avizului, în termen de 3 zile, MCSI va remite solicitantului un exemplar al avizului.
- (5) Avizul va fi eliberat conform modelului prezentat în anexa nr. 2.

Art. 14

(1) În situația în care, pe durata de valabilitate a avizului eliberat de MCSI, emitentul se înregistrează cu o nouă denumire în Registrul Comerțului și/sau în Registrul Bancar, acesta va notifica oficial MCSI, în termen de 30 de zile de la data înregistrării schimbării, pentru a i se elibera un nou aviz.

(2) În situația în care se va păstra aceeași denumire comercială a instrumentului de plată cu acces la distanță, documentele necesare pentru eliberarea noului aviz, care vor fi anexate la notificare, sunt:

a) cererea de înlocuire a avizului, adresată în acest scop MCSI, conform modelului prevăzut în anexa nr. 4;

b) noua licență de funcționare a emitentului, acordată de BNR, sau notificarea transmisă de autoritatea competentă din statul membru de origine către BNR;

c) copie după documentul eliberat de Registrul Comerțului și/sau Registrul Bancar, cu noua denumire a emitentului;

d) modelul noului contract prin care este oferit instrumentul de plată cu acces la distanță.

(3) În situația în care denumirea comercială a instrumentului de plată cu acces la distanță va fi modificată, după întreprinderea demersurilor prevăzute la alin (2) și primirea noului aviz, emitentul este obligat să reactualizeze toate documentele și procedurile proprii elaborate anterior, iar în termen de 60 de zile de la primirea noului aviz, să trimită la sediul MCSI un exemplar al documentației actualizate, conform prevederilor art. 7 și art. 12, alin (1).

(4) Noul aviz eliberat, conform modelului prezentat în anexa nr. 5, va fi valabil până la aceeași dată prevăzută în avizul eliberat anterior.

(5) În situația nerespectării perioadei de notificare prevăzută la alin. (1), MCSI poate decide suspendarea valabilității avizului eliberat, acțiune care obligă emitentul la oprirea imediată a funcționării instrumentului de plată cu acces la distanță al emitentului până la finalizarea demersurilor acestuia pentru obținerea noului aviz, respectiv la înștiințarea tuturor deținătorilor sau utilizatorilor autorizați cu privire la această suspendare a avizului și nefuncționării temporare a serviciilor puse la dispoziție prin intermediul instrumentului de plată cu acces la distanță.

CAPITOLUL III: Dispoziții finale

Art. 15

(1) În perioada prevăzută la art. 13 alin. (1), precum și în perioada de valabilitate a avizului sau în cazul primirii unei notificări din partea BNR, MCSI poate solicita emitentului efectuarea de verificări la sediul acestuia, prin personal desemnat prin ordin al ministrului comunicațiilor și societății informaționale.

(2) În cazul în care, în urma verificărilor efectuate, se constată nerespectarea prevederilor sau neaplicarea cerințelor procedurilor conținute în documentația de avizare, MCSI poate dispune neacordarea avizului sau retragerea acestuia.

Art. 16

(1) Emitentul este obligat să informeze MCSI, trimestrial, cu privire la numărul de utilizatori ai instrumentului de plată cu acces la distanță, numărul de plăți efectuate prin intermediul instrumentelor de plată cu acces la distanță, precum și valoarea plăților efectuate prin intermediul acestora, în formatul prezentat în anexa nr. 3.

(2) Numărul de utilizatori prevăzut la alin. (1) se referă la numărul de utilizatori cu care există încheiat un contract pentru utilizarea instrumentului de plată cu acces la distanță, pe parcursul trimestrului pentru care se face raportarea. Se iau în considerare toate contractele în vigoare de la data lansării instrumentului de plată cu acces la distanță.

(3) Numărul de plăți efectuate prin intermediul instrumentelor de plată cu acces la distanță se referă la plățile efectuate doar pe perioada trimestrului raportat și care vor fi prezentate, defalcat, în numărul de plăți în lei și în numărul de plăți în valută.

(4) Valoarea plăților efectuate prin intermediul instrumentelor de plată cu acces la distanță în perioada trimestrului raportat va fi prezentată astfel: valoarea plăților efectuate în lei și valoarea plăților efectuate în valută. Plățile efectuate în valută vor fi exprimate în echivalent euro, la cursul de schimb BNR din ultima zi a trimestrului pentru care se face raportarea.

(5) Raportările pot fi transmise prin poștă, pe adresa Ministerului Comunicațiilor și Societății Informaționale, B-dul Libertății nr. 14, Sectorul 5, cod 050706, București, sau prin e-mail criptat, ca fișier atașat, pe adresa e-banking@mcti.ro sau e-banking@mcsi.ro.

(6) Raportările vor fi transmise către MCSI până la sfârșitul lunii următoare trimestrului pentru care se face raportarea.

Art. 17

(1) Emitentul este obligat, pe perioada de valabilitate a avizului, să notifice MCSI în termen de 15 zile de la data înregistrării, despre:

a) apariția unor noi reglementări bancare cu aplicabilitate sau efecte asupra instrumentului de plată cu acces la distanță, schimbarea datelor de contact ale persoanelor responsabile, numelui persoanei sau a funcției care reprezintă legal emitentul, denumirii oficiale a emitentului etc., pentru a se actualiza datele și informațiile cuprinse în documentația de la sediul MCSI, trimisă anterior pentru eliberarea avizului;

b) retragerea din producție a instrumentul de plată cu acces la distanță;

(2) Emitentul este obligat, pe perioada de valabilitate a avizului, să notifice MCSI imediat (dar nu mai târziu de 24 de ore pe durata normală de lucru din timpul săptămânii) sau cel mai târziu în prima zi lucrătoare după sfârșitul de săptămână, sau după zilele declarate sărbători legale ori religioase, despre atacurile informatice care au afectat sau care au produs daune financiare și/sau de imagine atât emitentului cât și deținătorilor sau utilizatorilor autorizați ai instrumentului de plată cu acces la distanță.

(3) În situațiile prevăzute la alin. 2, MCSI poate decide suspendarea valabilității avizului eliberat, acțiune care obligă emitentul la eliminarea imediată și corectarea imediată a deficiențelor care au determinat luarea măsurii de suspendare a avizului, respectiv la înștiințarea tuturor deținătorilor sau utilizatorilor autorizați cu privire la această suspendare a avizului și nefuncționării temporare a serviciilor puse la dispoziție prin intermediul instrumentului de plată cu acces la distanță.

(4) Notificările emitentului, solicitate la alin. (1)-(3), vor fi transmise în aceeași modalitate ca și raportările trimestriale, conform prevederilor de la art. 16, alin. (5).

(5) După eliminarea sau corectarea deficiențelor și primirea din partea emitentului a notificării de remediere sau rezolvare a acestora, MCSI va ridica suspendarea valabilității avizului eliberat.

(6) În cazuri repetate a unor astfel de situații, MCTI poate decide retragerea avizului eliberat și înștiințarea, atât a emitentului, cât și a BNR, despre acest demers.

Art. 18

MCSI va lua măsurile ca, în cazul retragerii sau suspendării avizului acordat vreunui emitent, să transmită un comunicat de presă pentru informarea opiniei publice despre această acțiune, în conformitate cu prevederile Legii nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.

Art. 19

Eliberarea de către MCSI a avizului pentru furnizarea instrumentului de plată cu acces la distanță nu exonerează emitentul sau deținătorul instrumentului de răspunderile asumate prin contractul încheiat între aceștia, pe perioada funcționării și utilizării instrumentului de plată cu acces la distanță.

Art. 20

Anexele nr. 1-7 fac parte integrantă din prezentul ordin.

Art. 21

(1) Anexa nr. 6 va fi actualizată periodic (de regulă, o dată pe semestru) cu noile acte legislative și normative, reglementări și standarde în domeniul societății informaționale și securității sistemelor informatice, care au fost aprobate sau adoptate, respectiv cu cele care au fost abrogate, iar conținutul actualizat al acesteia va fi publicat prin grija MCSI pe site-ul oficial al ministerului (www.mcsi.ro) și va fi transmis persoanelor responsabile ale emitentului, dacă se solicită în mod expres acest lucru de către aceștia, la datele de contact specificate în documentația de avizare, conform prevederilor art. 8, alin. (1), pct. j).

(2) Actualizarea periodică a conținutului anexei nr. 6 nu implică modificarea prezentului ordin și republicarea acestuia în Monitorul Oficial al României, Partea I.

Art. 22

La data publicării prezentului ordin în Monitorul Oficial al României, Partea I, Ordinul ministrului comunicațiilor și tehnologiei informației nr. 389/2007 privind procedura de avizare a instrumentelor de plată cu acces la distanță, de tipul aplicațiilor internet-banking, home-banking sau mobile-banking, publicat în Monitorul Oficial al României, Partea I, nr. 485 din data de 19 iulie 2007, se abrogă.

Art. 23

Prezentul ordin va fi publicat în Monitorul Oficial al României, Partea I.

Ministrul comunicațiilor și societății informaționale,

CERERE
de eliberare a avizului

..... (denumirea emitentului), având sediul în
(adresa completă, inclusiv telefon și fax), înmatriculată/înregistrată la oficiul registrului comerțului sub
nr.(numărul de înregistrare, data înregistrării)....., cod fiscal/ cod unic de înregistrare
....., având Autorizația de funcționare nr., eliberată de Banca
Națională a României, reprezentată legal prin
(numele și prenumele), în calitate de (funcția)....., domiciliat(ă) în..... (adresa completă,
inclusiv telefon), identificat(ă) prin (actul de identitate: seria, numărul și emitentul,
precum și codul numeric personal), în conformitate cu prevederile Hotărârii Guvernului nr. 12
din 16 ianuarie 2009 privind organizarea și funcționarea Ministerului Comunicațiilor și Societății
Informaționale, prevederile art. 30, alin. B, lit. d) din Regulamentul nr. 6 din 11 octombrie 2006 emis
de Banca Națională a României privind emiterea și utilizarea instrumentelor de plată electronică și
relațiile dintre participanții la tranzacțiile cu aceste instrumente, publicat în Monitorul Oficial al
României, Partea I, nr. 927 din 15 noiembrie 2006, și prevederile Ordinului ministrului comunicațiilor
și societății informaționale nr. din data de, vă solicităm eliberarea avizului
pentru furnizarea instrumentului de plată cu acces la distanță(denumirea instrumentului)
....., cu următoarele caracteristici generale (scurtă descriere):

.....
.....
.....

Sistemul va funcționa/funcționează la sediul din

Numele, prenumele, funcția și ștampila solicitantului
Data

MODEL AVIZ

MINISTRUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE,

Având în vedere prevederile Hotărârii Guvernului nr. 12 din 16 ianuarie 2009 privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare,

Având în vedere prevederile Regulamentului nr. 6 din 11 octombrie 2006 emis de Banca Națională a României privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, publicat în Monitorul Oficial al României, Partea I, nr. 927 din 15 noiembrie 2006,

Având în vedere prevederile Ordinului ministrului comunicațiilor și societății informaționale nr., din data de,

eliberează prezentul

AVIZ

..... (denumirea emitentului), având sediul în (adresa poștală completă, inclusiv numere de telefon și fax), înmatriculată/înregistrată la oficiul registrului comerțului sub nr., cod fiscal/cod unic de înregistrare, având Autorizația de funcționare nr., eliberată de Banca Națională a României, reprezentat(ă) legal prin..... (numele și prenumele), în calitate de (funcția)....., a obținut avizul pentru furnizarea instrumentului de plată cu acces la distanță(denumirea instrumentului)....., cu următoarele caracteristici generale:

.....
.....
.....
.....
.....

Sistemul va funcționa/funcționează la sediul din

Observații:

Prezentul aviz s-a eliberat în vederea obținerii/menținerii autorizației pentru emiterea instrumentului de plată cu acces la distanță din partea Băncii Naționale a României și este valabil până la

Ministrul comunicațiilor și societății informaționale,

.....

Nr.....

Data.....

MODEL
Tabel pentru raportări trimestriale

Denumirea emitentului:

Denumirea instrumentului	Numărul de utilizatori	Numărul de tranzacții - lei -	Numărul de tranzacții - valută -	Valoarea tranzacțiilor - lei -	Valoarea tranzacțiilor în valută (echivalent EURO)	Perioada de raportare
						Trim. Anul

CERERE
de înlocuire a avizului

..... (denumirea actuală a emitentului), având sediul în (adresa completă, inclusiv telefon și fax), înmatriculată/înregistrată la oficiul registrului comerțului sub nr. (numărul de înregistrare, data înregistrării), cod fiscal/cod unic de înregistrare, având Autorizația de funcționare nr., eliberată de Banca Națională a României, reprezentată legal prin (numele și prenumele), în calitate de (funcția), domiciliat(ă) în..... (adresa completă, inclusiv telefon), identificat(ă) prin (actul de identitate: seria, numărul și emitentul, precum și codul numeric personal), în conformitate cu prevederile Hotărârii Guvernului nr. 12 din 16 ianuarie 2009 privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, prevederile art. 30, alin. B, lit. d) din Regulamentul nr. 6 din 11 octombrie 2006 emis de Banca Națională a României privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, publicat în Monitorul Oficial al României, Partea I, nr. 927 din 15 noiembrie 2006, și prevederile Ordinului ministrului comunicațiilor și societății informaționale nr. din data de, vă solicităm eliberarea unui nou aviz pentru înlocuirea avizului cu nr., eliberat la data de, pentru furnizarea instrumentului de plată cu acces la distanță(denumirea anterioară a instrumentului)....., de către (denumirea anterioară a emitentului), cu sediul în (adresa completă, inclusiv telefon și fax), înmatriculată/înregistrată la oficiul registrului comerțului sub nr. (numărul de înregistrare, data înregistrării), cod fiscal/cod unic de înregistrare, având Autorizația de funcționare nr., eliberată de Banca Națională a României, reprezentată legal prin (numele și prenumele), în calitate de (funcția) Menționăm că denumirea comercială a instrumentului de plată cu acces la distanță va rămâne aceeași/ se va modifica în (denumirea nouă a instrumentului de plată cu acces la distanță) Sistemul va funcționa/funcționează la sediul din

Numele, prenumele, funcția și ștampila solicitantului
Data

MODEL AVIZ ÎNLOCUIRE

MINISTRUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE,

Având în vedere prevederile Hotărârii Guvernului nr. 12 din 16 ianuarie 2009 privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare,

Având în vedere prevederile Regulamentului nr. 6 din 11 octombrie 2006 emis de Banca Națională a României privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, publicat în Monitorul Oficial al României, Partea I, nr. 927 din 15 noiembrie 2006,

Având în vedere prevederile Ordinului ministrului comunicațiilor și societății informaționale nr., din data de,

eliberează prezentul

AVIZ

.....(denumirea actuală a emitentului)....., având sediul în
(adresa poștală completă, inclusiv numere de telefon și fax), înmatriculată/înregistrată la oficiul
registruului comerțului sub nr., cod fiscal/cod unic de înregistrare, având
Autorizația de funcționare nr., eliberată de Banca Națională a României,
reprezentat(ă) legal prin..... (numele și prenumele), în calitate de
(funcția)....., a obținut avizul pentru furnizarea instrumentului de plată cu acces la distanță
.....(denumirea actuală a instrumentului)....., cu următoarele caracteristici generale:

.....
.....
.....
.....
.....

Sistemul va funcționa/funcționează la sediul din

Observații:

Prezentul aviz, care înlocuiește avizul cu numărul, eliberat la data, obținut anterior de
..... (denumirea anterioară a emitentului)....., cu sediul în, pentru
instrumentul de plată cu acces la distanță (denumirea anterioară a instrumentului), s-a
eliberat în vederea obținerii/menținerii autorizației pentru emiterea instrumentului de plată cu acces la
distanță din partea Băncii Naționale a României și este valabil până la (aceeași perioadă
prevăzută în avizul anterior)

Ministrul comunicațiilor și societății informaționale,

.....

Nr.....

Data.....

LISTA
cu acte legislative și normative, reglementări și standarde în vigoare,
în domeniul societății informaționale, securității sistemelor informatice și în domeniul bancar

1. Ordinul ministrului comunicațiilor și tehnologiei informației nr. CCC din ZZ LLL 2009 (OMCTI CCC/2009) privind procedura de avizare a instrumentelor de plată cu acces la distanță, de tipul aplicațiilor internet-banking, home-banking sau mobile-banking.
2. Regulamentul Băncii Naționale a României (BNR) nr. 6 din 11.10.2006 privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente.
3. Legea nr. 365 din 7 iunie 2002 privind comerțul electronic, modificată prin Legea nr. 121 din 4 mai 2006 pentru modificarea și completarea Legii nr. 365/2002 privind comerțul electronic.
4. Legea nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
5. Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (abrogă Legea 676/2001).
6. Legea nr. 8 din 14 martie 1996 privind dreptul de autor și drepturile conexe, cu modificările aduse prin Legea nr. 285/2004, Ordonanța de Urgență 123/2005 și Legea 329/2006.
7. Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
8. Legea nr. 455 din 18 iulie 2001 privind semnătura electronică.
9. Hotărârea Guvernului nr. 1.259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică.
10. Legea nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției.
11. Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.
12. Hotărârea Guvernului nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România.
13. Hotărârea Guvernului nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
14. Legea nr. 135 din 15 mai 2007 privind arhivarea documentelor în formă electronică, publicată în Monitorul Oficial, Partea I, nr. 345 din 22 mai 2007.
15. Decizia Autorității Naționale pentru Comunicații (ANC) nr. 1131/2008 privind normele metodologice de autorizare a centrelor de date, publicată în Monitorul Oficial, Partea I, nr. 861 din 20.12.2008.
16. Regulamentul BNR nr. 3/1997 privind efectuarea operațiunilor valutare.
17. Regulamentul BNR nr. 1/1995 privind principiile și organizarea avizării tehnice a sistemelor de plăți și decontări fără numerar.
18. Regulamentul BNR nr. 5/2006 privind regimul valutar.
19. Regulamentul BNR nr. 2/2005 privind ordinul de plată utilizat în operațiuni de transfer credit.
20. Convenția Consiliului Europei din 23.11.2001 privind criminalitatea informatică.
21. Legea nr. 845/2003 pentru modificarea și completarea Legii Bancare nr. 58/1998.
22. Legea nr. 58/1998 – legea bancară și păstrarea secretului bancar.
23. Legea nr. 36/01.03.2006 pentru aprobarea Ordonanței de Urgență a Guvernului nr. 135/2005 privind modificarea Legii nr. 656/2002 pentru prevenirea și sancționarea spălării banilor,

- precum și pentru instituirea unor măsuri de prevenire și combatere a finanțării actelor de terorism publicată în Monitorul Oficial nr. 200 din 3 martie 2006.
24. OUG nr. 99/2006 privind instituțiile de credit și adecvarea capitalului.
 25. Ordonanța nr. 6/2004 privind transferurile transfrontaliere.
 26. Norma 1/2005 privind modul unitar de completare a mențiunilor din ordinele de plată în mesajele electronice utilizate în sistemul ReGIS (RTGS) și în casa de compensare automată.
 27. Reguli de sistem ale SENT (ACH).
 28. Normele cadru BNR nr. 9/1996 privind executarea ordinelor de plată programate.
 29. Standardul internațional ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.
 30. Standardul internațional ISO/IEC TR 13335-2:1997, Information technology . Guidelines for the management of IT Security . Part 2: Managing and planning IT Security.
 31. Standardul internațional ISO/IEC TR 13335-3:1998, Information technology . Guidelines for the management of IT Security . Part 3: Techniques for the management of IT Security.
 32. Standardul internațional ISO/IEC TR 13335-4:2000, Information technology . Guidelines for the management of IT Security . Part 4: Selection of safeguards.
 33. Standardul internațional ISO/IEC 13888-1:1997, Information technology . Security techniques . Non-repudiation . Part 1: General.
 34. Standardul internațional ISO/IEC 13888-2:1998, Information technology . Security techniques . Non-repudiation . Part 2: Mechanisms using symmetric techniques.
 35. Standardul internațional ISO/IEC 13888-3:1997, Information technology . Security techniques . Non-repudiation . Part 3: Mechanisms using asymmetric techniques.
 36. Standardul internațional SR ISO/CEI TR 14516. Tehnologia informației – Tehnici de securitate – Îndrumări pentru utilizarea și administrarea serviciilor părților terțe de încredere.
 37. Standardul național SR ISO/CEI 15408-1:2004. Tehnologia informației - Tehnici de securitate - Criterii de evaluare pentru securitatea tehnologiei informației - Partea 1: Introducere și model general.
 38. Standardul național SR ISO/CEI 15408-2:2005. Tehnologia informației - Tehnici de securitate - Criterii de evaluare pentru securitatea tehnologiei informației - Partea 2: Cerințe funcționale de securitate.
 39. Standardul național SR ISO/CEI 15408-3:2005. Tehnologia informației - Tehnici de securitate - Criterii de evaluare pentru securitatea tehnologiei informației - Partea 3: Cerințe pentru asigurarea securității.
 40. Standardul internațional ISO/IEC TR 15443-1. Information technology — Security techniques — A framework for IT security assurance — Part 1: Overview and framework.
 41. Standardul internațional ISO/IEC TR 15443-2. Information technology — Security techniques — A framework for IT security assurance — Part 2: Assurance methods.
 42. Standardul internațional ISO/IEC TR 15443-3. Information technology — Security techniques — A framework for IT security assurance — Part 3: Analysis of assurance methods.
 43. Standardul național SR ISO/CEI 15939. Inginerie software – Proces de măsurare a software-ului.
 44. Standardul internațional ISO/IEC 17021:2006, Conformity assessment — Requirements for bodies providing audit and certification of management systems
 45. Standardul național SR ISO/CEI 18014-1. Tehnologia informației – Tehnici de securitate - Servicii de marcare temporală – Partea 1: Cadru general.
 46. Standardul național SR ISO/CEI 18014-2. Tehnologia informației – Tehnici de securitate - Servicii de marcare temporală – Partea 2: Mecanisme care produc mărci temporale independente.

47. Standardul național SR ISO/CEI 18014-3. Tehnologia informației – Tehnici de securitate - Servicii de marcare temporală – Partea 3: Mecanisme care produc mărci temporale înlănțuite.
48. Standardul internațional ISO/IEC 18028-2:2005, Information technology — Security techniques — IT network security — Part 1: Network security management.
49. Standardul internațional ISO/IEC 18028-2:2005, Information technology — Security techniques — IT network security — Part 2: Network security architecture.
50. Standardul internațional ISO/IEC 18028-3:2005, Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways.
51. Standardul internațional ISO/IEC 18028-4:2005, Information technology — Security techniques — IT network security — Part 4: Securing remote access
52. Standardul internațional ISO/IEC 18028-5:2006, Information technology — Security techniques — IT network security — Part 5: Securing communications across networks using virtual private networks.
53. Standardul internațional ISO/IEC 18043:2006, Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems.
54. Standardul internațional ISO/IEC 18044:2004, Information technology — Security techniques — Information security incident management.
55. Standardul internațional ISO/IEC 20000-1:2005, Information technology — Service management — Part 1: Specification.
56. Standardul internațional ISO/IEC 20000-2:2005, Information technology — Service management — Part 2: Code of practice.
57. Standardul național SR ISO/CEI 23026:2006. Inginerie software. Practici recomandate pentru construcția, managementul și ciclul de viață a sit-urilor web.
58. Standardul internațional ISO/IEC 24762:2008 Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services
59. Standardul internațional ISO/IEC 27001:2005, respectiv Standardul național SR ISO/CEI 27001:2006 Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe.
60. Standardul național SR ISO/IEC 27002:2005. Tehnologia Informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației.
61. Standardul internațional ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management.
62. Standardul național SR ISO/CEI 27006:2007. Tehnologia Informației. Tehnici de securitate. Cerințe pentru organismele care furnizează audit și certificare pentru sistemele de management a securității informației.
63. Standardul internațional ISO/IEC 38500:2008. Corporate governance of information technology.
64. Standardul național SR ISO/CEI 9126-1. Inginerie software. Calitatea produsului. Partea 1: Modelul calității.
65. Standardul internațional ISO/IEC TR 9126-2:2003. Software engineering -- Product quality -- Part 2: External metrics.
66. Standardul internațional ISO/IEC TR 9126-3:2003. Software engineering -- Product quality -- Part 3: Internal metrics.
67. Standardul internațional ISO/IEC TR 9126-4:2004. Software engineering -- Product quality -- Part 4: Quality in use metrics.
68. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. September 2006, Version 3.1, Revision 1.
69. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. September 2007, Version 3.1, Revision 2.

70. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. September 2007, Version 3.1, Revision 2.
71. Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules.
72. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program.
73. Ordine ale Directorului General al Oficiului Registrului Național al Informațiilor Secrete de Stat (ORNISS) privind protecția informațiilor clasificate:
 - a. ORDINUL nr. 482 din 21 noiembrie 2003 pentru aprobarea Directivei privind structurile cu responsabilități în domeniul INFOSEC - INFOSEC 1.
 - b. ORDINUL nr. 483 din 21 noiembrie 2003 pentru aprobarea Directivei principale privind domeniul INFOSEC - INFOSEC 2.
 - c. ORDINUL nr. 484 din 21 noiembrie 2003 pentru aprobarea Directivei privind managementul INFOSEC pentru sisteme informatice și de comunicații - INFOSEC 3.
 - d. ORDINUL nr. 485 din 21 noiembrie 2003 privind aprobarea Directivei INFOSEC tehnice și de implementare pentru interconectarea sistemelor informatice și de comunicații (SIC) - INFOSEC 7.
 - e. ORDINUL nr. 486 din 21 noiembrie 2003 privind aprobarea Instrucțiunilor pentru controlul și protecția materialelor COMSEC NATO în statele nemembre NATO și organizațiile internaționale - IC 1.
 - f. ORDINUL nr. 487 din 21 noiembrie 2003 privind aprobarea Directivei INFOSEC tehnice și de implementare a securității criptografice și a mecanismelor criptografice NATO - IC 3.
 - g. ORDINUL nr. 488 din 21 noiembrie 2003 privind aprobarea Ghidului pentru elaborarea documentației cu cerințele de securitate (DCS) pentru sisteme informatice și de comunicații (SIC) - DS 1.
 - h. ORDINUL nr. 489 din 21 noiembrie 2003 pentru aprobarea Ghidului privind structura și conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice și de comunicații (SIC) - DS 2.
 - i. ORDINUL nr. 490 din 21 noiembrie 2003 pentru aprobarea Ghidului pentru instalarea echipamentelor electronice destinate prelucrării informațiilor clasificate - DS 6.
 - j. ORDINUL nr. 386 din 11 noiembrie 2004 pentru aprobarea Ghidului pentru acreditarea de securitate a sistemelor informatice și de comunicații naționale care vehiculează informații NATO - DS 8.
 - k. ORDINUL nr. 387 din 11 noiembrie 2004 pentru aprobarea Ghidului INFOSEC tehnic și de implementare pentru protejarea sistemelor informatice și de comunicații împotriva programelor informatice nocive - DS 9.
 - l. ORDINUL nr. 388 din 11 noiembrie 2004 pentru aprobarea Directivei INFOSEC tehnice și de implementare privind securitatea transmisiilor - INFOSEC 10.
 - m. ORDINUL nr. 389 din 11 noiembrie 2004 pentru aprobarea Metodologiei privind managementul riscului de securitate pentru sistemele informatice și de comunicații care stochează, procesează sau transmit informații clasificate - DS 3.
 - n. ORDINUL nr. 390 din 11 noiembrie 2004 pentru aprobarea Directivei INFOSEC tehnice și de implementare privind cerințele instrumentelor de securitate, selectarea, aprobarea și implementarea acestora - INFOSEC 9.
 - o. ORDINUL nr. 391 din 11 noiembrie 2004 pentru aprobarea Directivei INFOSEC tehnice și de implementare privind securitatea calculatoarelor și a rețelelor locale - INFOSEC 4.
 - p. ORDINUL nr. 3 din 5 ianuarie 2005 pentru aprobarea Ghidului INFOSEC privind analiza naturii și proporțiilor amenințărilor și vulnerabilităților la adresa sistemelor informatice și de comunicații (SIC) - DS 4.
 - q. ORDINUL nr. 4 din 5 ianuarie 2005 pentru aprobarea Ghidului general de securitate a sistemelor informatice și de comunicații - DS 5.

- r. ORDINUL nr. 149 din 18 aprilie 2005 pentru aprobarea Metodologiei privind elaborarea Planului pentru continuarea activității în situații de urgență pentru sisteme informatice și de comunicații (SIC) care vehiculează informații clasificate - DS 7.
- s. ORDINUL nr. 5 din 12 ianuarie 2006 pentru aprobarea Instrucțiunilor privind transportul materialelor NATO clasificate AC-1.
- t. ORDINUL nr. 11 din 26 ianuarie 2006 pentru aprobarea Directivei INFOSEC privind Catalogul național cu produse, profile și pachete de protecție INFOSEC - INFOSEC 5.
- u. ORDINUL nr. 12 din 27 ianuarie 2006 pentru aprobarea Metodologiei privind acreditarea structurilor interne INFOSEC din cadrul autorităților desemnate de securitate - INFOSEC 11.
- v. ORDINUL nr. 13 din 31 ianuarie 2006 pentru aprobarea normelor cadru privind securitatea fizică a informațiilor UE clasificate. Anexă: Normele cadru privind securitatea fizică a informațiilor UE clasificate.
- w. ORDINUL nr. 160 din 06 februarie 2006 pentru aprobarea normelor cadru privind securitatea informațiilor UE clasificate. Anexă: Normele cadru privind securitatea informațiilor UE clasificate.
- x. ORDINUL nr. 159 din 6 februarie 2006 pentru aprobarea Directivei INFOSEC tehnice și de implementare privind securitatea emisiei - INFOSEC 6.
- y. ORDINUL nr. 167 din 27 februarie 2006 pentru aprobarea Metodologiei de acreditare a entităților pentru evaluarea produselor de securitate IT și a sistemelor informatice și de comunicații - INFOSEC 12.
- z. ORDINUL nr. 172 din 10 martie 2006 pentru aprobarea Directivei privind acreditarea de securitate a sistemelor informatice și de comunicații (SIC) care stochează, procesează sau transmit informații naționale clasificate - INFOSEC 13.
- aa. ORDINUL nr. 181 din 13 aprilie 2006 pentru aprobarea Metodologiei de evaluare și certificare a produselor, profilelor și pachetelor de protecție INFOSEC - INFOSEC 14.
- bb. ORDINUL nr. 171 din 10 martie 2006 pentru aprobarea Ghidului INFOSEC privind estimarea nivelurilor de încredere pentru medii specifice în care operează sisteme informatice și de comunicații - DS 13.
- cc. ORDINUL nr. 170 din 10 martie 2006 pentru aprobarea Ghidului de securitate privind sistemul de operare Windows 2000 Server - DS 17.
- dd. ORDINUL nr. 174 din 16 martie 2006 pentru aprobarea Ghidului INFOSEC tehnic și de implementare privind centralele telefonice automate de comutație - DS 10.
- ee. ORDINUL nr. 192 din 29 mai 2006 privind aprobarea procedurii de acreditare, desființare sau reacreditare a Componentelor Sistemului Național de Registre. Anexă: Procedura de acreditare, desființare sau reacreditare a Componentelor Sistemului Național de Registre.
- ff. ORDINUL nr. 471 din 21 decembrie 2007 pentru aprobarea Procedurii naționale de lucru privind zona TEMPEST a locațiilor.
- gg. ORDINUL nr. 171 din 19 iunie 2008 privind modificarea Metodologiei de evaluare și certificare a produselor, profilelor și pachetelor de protecție INFOSEC-INFOSEC 14.
- hh. Ordinul nr. 198 din 7 august 2008 pentru aprobarea Ghidului INFOSEC tehnic și de implementare privind identificarea și autentificarea în sistemele informatice și de comunicații care vehiculează informații clasificate - DS 11.
- ii. Ordinul nr. 199 din 7 august 2008 pentru aprobarea Politicii de interconectare a sistemelor informatice și de comunicații care vehiculează informații UE clasificate - INFOSEC 8.

74.Recomandări ale Internet Engineering Task Force (IETF) – tip Request For Comments (RFC) în mediul Internet.

75.Recomandări ale International Telecommunication Union (ITU).

MODEL NOTIFICARE

Către: **Banca Națională a României**
Str. Lipscani nr.25, București
Fax: 312.62.61

In atenția, Director al Direcției Reglementare și Autorizare

Stimată/e Doamnă/Domnule Director,

Prin prezenta vă comunicăm că în perioada –, Ministerul Comunicațiilor și Societății Informaționale (MCSI) a emis de avize pentru instrumente de plată cu acces la distanță (..... avize pentru menținerea și avize pentru obținerea aprobării Băncii Naționale a României) - în conformitate cu prevederile Regulamentului Băncii Naționale a României (BNR) nr. 6 din 11.10.2006 privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente și ale Ordinul ministrului comunicațiilor și tehnologiei informației nr. CCC din ZZ LLL 2009 (OMCTI CCC/2009) privind procedura de avizare a instrumentelor de plată cu acces la distanță, de tipul aplicațiilor internet-banking, home-banking sau mobile-banking, conform situației din tabelul nr.1 :

Nr. crt.	Denumire instituție bancară	Denumire instrument	Tip instrument	Număr aviz, Data eliberării, Obținere/ menținere aprobare BNR	Valabilitate aviz

Tabelul nr. 1

NOTĂ: După expirarea perioadei de înaintare a documentațiilor de avizare la sediul MCSI, conform prevederilor art. 9, alin. 1 din Ordinul ministrului comunicațiilor și societății informaționale nr. din data de, au solicitat reavizarea instrumentelor de plată aflate în producție toate instituțiile bancare / n-au solicitat reavizarea instrumentelor de plată aflate în producție un număr de instituții bancare, conform situației din tabelul nr. 2:

Nr. crt.	Denumire instituție bancară	Denumire instrument	Tip instrument

Tabelul nr. 2

**Funcția,
Numele și prenumele directorului structurii din MCSI
Semnătura și ștampila**