Eesti Panga presidendi
15. novembri 2010. a määruse nr 18
„„TARGET2-Eesti reeglite kinnitamine"
muutmine"
lisa
Eesti Panga presidendi
9. mai 2008. a määruse nr 4
„TARGET2-Eesti reeglite kinnitamine"
lisa 2

Internetipõhiseks juurdepääsuks vajalikud täiendused ja muudatused TARGET2-Eestis osalemise ühtsetes tingimustes

Artikkel 1 – **Kohaldamisala**

Ühe või mitme maksemoodulikonto internetipõhist juurdepääsu kasutavate osalejate suhtes kohaldatakse Eesti Panga presidendi 2008. aasta 9. mai määruse nr 4 „TARGET2-Eesti reeglite kinnitamine" (edaspidi *määrus*) lisas 1 „TARGET2-Eestis osalemise ühtsed tingimused" (edaspidi *lisa 1* või *ÜT*) määratletud tingimusi kooskõlas käesoleva lisa (edaspidi ka *lisa 2*) sätetega.

Artikkel 2 – **Mõisted**

Käesolevas lisas kasutatakse peale lisas 1 määratletud mõistete järgmisi mõisteid:

elektroonilised sertifikaadid või *sertifikaadid* (*electronic certificates*, *certificates*) – sertifitseerimisasutuse väljastatud elektrooniline andmefail, mis seob avaliku võtme isikuga ning mida kasutatakse avaliku võtme asjaomasele isikule kuuluvuse kontrollimiseks; omaniku isiku tuvastamiseks; isiku allkirja kontrollimiseks või isikule adresseeritud sõnumi krüpteerimiseks. Sertifikaadid on salvestatud füüsilisele andmekandjale, näiteks kiipkaardile või mälupulgale, ning viide sertifikaadile tähendab ka viidet asjaomasele andmekandjale. Sertifikaadid on olulised internetipõhiselt TARGET2-e kasutavate ja maksesõnumeid või kontrollsõnumeid saatvate osalejate isiku tuvastamiseks;

internetipõhine juurdepääs (*Internet-based access*) – osaleja on valinud maksemooduli konto, millele on juurdepääs ainult interneti kaudu, ja osaleja saadab maksesõnumeid või kontrollsõnumeid TARGET2-le interneti kaudu;

internetiteenuse osutaja (*Internet service provider*) – ettevõte või organisatsioon (*gateway*), mille kaudu TARGET2 osaleja kasutab internetipõhise juurdepääsuga TARGET2 kontot;

sertifikaadi omanik (*certificate holder*) – konkreetne indiviid, kelle isikusamasuse on tuvastanud TARGET2 osaleja ning kellele TARGET2 osaleja on andnud volituse omada internetipõhist juurdepääsu osaleja TARGET2 kontole. Avaldus sertifikaadi saamiseks peab olema kinnitatud osaleja asukohariigi keskpanga (RKP) poolt ning edastatud sertifitseerimisasutusele, kes omakorda väljastab sertifikaadi, mis seob avaliku võtme osaleja isikut tõendavate dokumentidega;

sertifitseerimisasutused (*certification authorities*) – üks või mitu EKP nõukogu poolt elektrooniliste sertifikaatide väljastamisel, haldamisel, tagasivõtmisel ja uuendamisel eurosüsteemi nimel tegutsema määratud RKPd.

Artikkel 3 – **Mittekohaldatavad sätted**

Internetipõhisele juurdepääsule ei kohaldata järgmisi lisa 1 sätteid: artikli 4 lõike 1 punkt c ja lõike 2 punkt d; artikli 5 lõiked 2, 3 ja 4; artiklid 6 ja 7; artikli 11 lõige 8; artikli 14 lõike 1 punkt a; artiklid 23–26; artikkel 41 ning I, VI ja VII liide.

Artikkel 4 – **Täiendatud ja muudetud sätted**

Internetipõhisele juurdepääsule kohaldatakse lisa 1 sätteid järgmises sõnastuses:
1) artikli 2 lõige 1:
„(1) Järgmised liited on ÜT lahutamatu osa ning neid kohaldatakse maksemooduli kontole internetipõhist juurdepääsu kasutavatele osalejatele:
lisa 2 IA liide: maksejuhiste töötlemise tehniline kirjeldus internetipõhiseks juurdepääsuks
lisa 2 IIA liide: internetipõhise juurdepääsu tasud ja arved
II liide: TARGET2 hüvitussüsteem
III liide: õigusvõime hinnangu ja õiguskeskkonna hinnangu nõuded
IV liide: talitluspidevuse ja eriolukorra meetmed, v.a punkti 7 alapunkt b
V liide: töökorralduse ajakava”;
2) artikli 3 lõiked 4 ja 6:
„(4) Eesti Pank osutab teenuseid ÜT kohaselt. Ühisplatvormi käitavate keskpankade ja/või sertifitseerimisasutuste tegevus ja tegevusetus loetakse Eesti Panga tegevuseks ja tegevusetuseks, mille eest ta vastutab kooskõlas ÜT artikliga 31. Osalemisest ÜT kohaselt ei teki lepingulist suhet osalejate ja ühisplatvormi käitavate keskpankade vahel, kui viimased tegutsevad selles pädevuses. Korraldused, teated või teave, mille osaleja saab ühisplatvormi käitajalt või saadab talle seoses ÜT alusel osutatavate teenustega, loetakse saaduks Eesti Pangalt või saadetuks Eesti Pangale.
(6) Osalemine TARGET2s teostub osalemise teel TARGET2 osasüsteemis. ÜT kirjeldab TARGET2-Eesti osalejate ja Eesti Panga õigusi ja kohustusi. Maksejuhiste töötlemise eeskirjad (IV jaotis) hõlmavad iga TARGET2 osaleja kõiki maksejuhiseid või saadud makseid ning neid kohaldatakse lisa 2 kohaselt.”;
3) artikli 4 lõike 2 punkt e:
„e) krediidiasutused või punktides a–c osutatud mis tahes üksused, kui need on asutatud riigis, kellega liit on sõlminud valuutalepingu, mille kohaselt neil üksustel on juurdepääs liidu maksesüsteemidele valuutalepingus sätestatu kohaselt ning tingimusel, et nende asukohariigi õiguskord on võrdväärne vastavate liidu õigusaktidega.”;
4) artikli 8 lõike 1 algusest kuni punkti a alapunktini i (kaasa arvatud):
„(1) Internetipõhise juurdepääsuga maksemooduli konto avamiseks TARGET2-Eestis peab taotleja:
a) täitma järgmised tehnilised nõuded:
i) installeerima, haldama ja käitama vajaliku TARGET2-Eestiga ühendatud infotehnoloogia infrastruktuuri, jälgima ja tagama selle turvalisust ning sisestama selle kaudu maksejuhiseid lisa 2 IA liites sätestatud tehniliste nõuete kohaselt. Seda tehes võivad osalejad kasutada kolmandaid isikuid, jäädes ise täielikult vastutavaks; ja”;
5) artikli 8 lõike 1 täiendav punkt c:
„c) avaldama soovi kasutada maksemooduli kontot interneti vahendusel ning esitama avalduse eraldi maksekonto loomiseks TARGET2s, kui taotleja soovib lisaks juurdepääsu TARGET2-le võrguteenuse osutaja kaudu. Taotleja peab esitama korrektselt täidetud avalduse TARGET2-le internetipõhiseks juurdepääsuks tarvilike elektrooniliste sertifikaatide väljastamiseks.”;
6) artikli 9 lõiked 3 ja 5:
„(3) Internetipõhist juurdepääsu kasutavad osalejad võivad TARGET2 kataloogi vaadata vaid internetis; kataloogi majasisene või majaväline jagamine on keelatud.
(5) Osalejad nõustuvad, et Eesti Pank ja teised keskpangad võivad avaldada osalejate nimed ja ettevõtte tunnuskoodid.”

7) artikli 10 lõiked 1, 2 ja 5:

„(1) Eesti Pank pakub käesolevas lisas kirjeldatud internetipõhist juurdepääsu. Kui ÜTs või kehtivas õiguses ei ole sätestatud teisiti, peab Eesti Pank kasutama oma kohustuste täitmiseks kõiki tema käsutuses olevaid mõistlikke võimalusi, võtmata kohustust tagada tulemuse saavutamine.

(2) TARGET2 internetipõhist juurdepääsu kasutavad osalejad peavad maksma tasu lisa 2 IIA liite sätete kohaselt.

(5) Osalejad on kohustatud:

a) kogu tööpäeva jooksul korrapäraselt kontrollima ICMi laekunud informatsiooni, eelkõige teavet, mis puudutab olulisi süsteemisündmusi (näiteks kõrvalsüsteemi arveldusi puudutavad sõnumid) ja osaleja väljaarvamist või osaluse peatamist. Eesti Pank ei vastuta mis tahes otsese ega kaudse kahju eest, mis on tekkinud sellest, et osaleja pole kontrolli läbi viinud; ja

b) tagama lisa 2 liites IA sätestatud turvanõuete täitmise igal hetkel, eelkõige mis puudutab sertifikaatide turvalist hoidmist, ning rakendama eeskirju ja menetlusi, et tagada sertifikaatide omanike teadlikkus sertifikaatide turvalise hoidmise kohustuslikkusest.”;

8) artikli 11 lõiked 5a ja 6:

„(5a) Osalejad on kohustatud õigeaegselt ajakohastama TARGET2-le internetipõhiseks juurdepääsuks tarvilike elektrooniliste sertifikaatide väljastamise vormid ning esitama uued elektrooniliste sertifikaatide väljastamise vormid Eesti Pangale. Osalejad peavad kontrollima TARGET2-Eestisse sisestatud ja neid puudutava teabe õigsust.

(6) Eesti Pank loetakse pädevaks edastama sertifitseerimisasutustele osalejate kohta mis tahes teavet, mida sertifitseerimisasutused vajavad.”;

9) artikli 12 lõige 5

„(5) Eesti Pank teeb igapäevase kontoülevaate kättesaadavaks igale osalejale, kes on seda teenust soovinud.”;

10) artikli 13 punkt b:

„b) otsedebiteerimise volituse alusel saadud otsedebiteerimise korraldused. Otsedebiteerimise korraldusi ei saa maksemooduli kontolt esitada internetipõhist juurdepääsu kasutavad osalejad; ja”;

11) artikli 14 lõike 1 punkt b:

„b) maksesõnum vastab TARGET2-Eesti vorminõuetele ja tingimustele ning on läbinud lisa 2 IA liites kirjeldatud unikaalsuse kontrolli, ja”;

12) artikli 18 lõige 3:

„(3) Kui kasutatakse hiliseima debiteerimise aja määrangut, lükatakse maksejuhis tagasi, kui seda ei saa määratud debiteerimistähtajal arveldada. Viisteist minutit enne määratud debiteerimistähtaega teavitatakse maksealgatajat eelistatavalt ICMi kaudu; kui see pole võimalik või mõistlik, saadetakse ICMi kaudu automaatteade. Maksealgataja võib kasutada debiteerimise lõpptähtaja määrangut ka ainult hoiatusmääranguna. Sellistel juhtudel ei lükata vastavat maksejuhist tagasi.”;

13) artikli 21 lõige 4:

„(4) Maksja taotlusel võib Eesti Pank otsustada muuta erakorralise kiirmaksejuhise kohta järjekorras (v.a erakorralised maksejuhised arvelduskordades nr 5 ja 6), kui see muutus ei mõjuta kõrvalsüsteemi sujuvat arveldamist TARGET2s või ei tekita muul viisil süsteemiriski.”;

14) artikli 28 lõige 1 ja täiendav lõige 4:

„(1) Internetipõhist juurdepääsu kasutavad osalejad rakendavad asjakohast turvakontrolli, eelkõige lisa 2 IA liites nimetatud kontrolli, et kaitsta oma süsteeme lubamatu juurdepääsu ja kasutamise eest. Osalejad on ainuvastutavad oma süsteemide konfidentsiaalsuse, usaldusväärsuse ja kättesaadavuse piisava kaitse eest.

(4) Internetipõhist juurdepääsu kasutavad osalejad teavitavad Eesti Panka viivitamata sündmustest, mis võivad mõjutada sertifikaatide kehtivust, eelkõige lisa 2 IA liites nimetatud sündmustest, sealhulgas kõigist kahjudest või väärkasutusest.”;

15) artikkel 29:

„(1) ICM võimaldab järgmist:

a) maksete sisestamine osalejate poolt;

b) osalejate juurdepääs teabele nende kontode kohta ja likviidsuse juhtimine;

c) likviidsuse ülekandmise korralduste algatamine;
d) juurdepääs süsteemisõnumitele.

(2) ICMi täpsem tehniline kirjeldus seoses internetipõhise juurdepääsuga on esitatud lisa 2 liites 1A.";

16) artikli 32 lõiked 1 ja 3:

„(1) Kui ÜT ei sätesta teisiti, tehakse kõik maksetega ja maksete töötlemisega seotud TARGET2 puudutavad sõnumid, näiteks debiteerimise ja krediteerimise kinnitused või kontoväljavõtted Eesti Panga ja osalejate vahel, osalejale kättesaadavaks ICMis.

(3) Kui osaleja ühendus ei tööta, kasutab osaleja sõnumite edastamise alternatiivseid viise, mis on määratletud lisa 2 IA liites. Sellistel juhtudel käsitletakse tõendina sõnumi Eesti Panga poolt salvestatud või trükitud versiooni.";

17) artikli 34 lõike 4 punkt c:

„c) Sellise ICMi teate internetipõhist juurdepääsu kasutavatele osalejatele kättesaadavaks tegemisel loetakse, et asjaomaseid osalejaid on osaleja osaluse lõpetamisest/peatamisest TARGET2-Eestis või teises TARGET2 osasüsteemis teavitatud. Osalejad vastutavad kahju eest, mis tekib osalejatele, kelle osalus on peatatud või lõpetatud, määratud maksejuhise edastamisest, kui selline maksejuhis on sisestatud TARGET2-Eestisse pärast ICMi teate kättesaadavaks tegemist.";

18) artikli 39 lõige 1:

„(1) Eeldatakse, et osalejad teavad ja järgivad kõiki oma kohustusi, mis tulenevad andmekaitset ning rahapesu ja terrorismi rahastamise tõkestamist, massihävitusrelvade leviku tõkestamise seisukohast tundlikku tuumaenergiaalast tegevust või tuumarelva kandevahendite väljatöötamist reguleerivatest õigusaktidest, eelkõige rakendades asjakohaseid meetmeid seoses nende makse-mooduli kontodel debiteeritavate ja krediteeritavate summadega. Enne internetiteenuse osutajaga lepingu sõlmimist peavad internetipõhist juurdepääsu kasutavad osalejad tutvuma internetiteenuse osutaja andmekogumispõhimõtetega.";

19) artikli 40 lõige 1:

„(1) Kui ÜTs ei ole sätestatud teisiti, edastatakse kõik ÜT kohaselt nõutavad või lubatavad teated tähitud kirjaga, faksiga või kirjalikult. Teated Eesti Pangale edastatakse Eesti Panga arvelduste osakonna juhatajale aadressil Estonia pst 13, Tallinn või EPBEEE2X aadressil. Teated osalejale saadetakse osaleja aadressil või faksinumbril või BIC aadressil, nagu osaleja on Eesti Pangale avaldanud.";

20) artikkel 45:

„Artikkel 45 – Sätete eraldi kohaldatavus

ÜT või lisa 2 ühe või mitme sätte kehtetuks tunnistamine ei mõjuta ÜT või lisa 2 muude sätete kohaldatavust."

IA liide

Maksejuhiste töötlemise tehniline kirjeldus internetipõhiseks juurdepääsuks

Lisaks ÜT-le kohaldatakse maksejuhiste internetipõhise juurdepääsuga töötlemisele järgmisi reegleid:

1. Infrastruktuuri, võrgu ja vormingute tehnilised nõuded TARGET2-Eestis osalemiseks

(1) Iga internetipõhist juurdepääsu kasutav osaleja peab looma ühenduse TARGET2 ICMiga, kasutades kasutaja üksikasjaliku funktsioonikirjelduse (UDFS) lisas „Internetipõhine osalemine – internetiühenduse süsteeminõuded" sätestatud kohalikku klienti, operatsioonisüsteemi ja veebilehitsejat määravaid seadistusi. Iga osaleja maksemooduli konto tuvastatakse 8- või 11-kohalise BIC tunnuskoodi abil. Lisaks peab iga osaleja läbima testide seeria ning tõendama oma tehnilist ja töökorralduslikku valmisolekut, enne kui ta võib osaleda TARGET2-Eestis.
(2) Maksemoodulis maksejuhiste andmiseks ja maksesõnumite vahetamisel kasutatakse sõnumite saatja/vastuvõtjana TARGET2 platvormi BIC, TRGTXEPMLVP. Internetipõhist ühendust kasutavale osalejale saadetud maksejuhises peab asjaomase osaleja nimi olema märgitud makse saaja real. Internetipõhist ühendust kasutava osaleja antud maksejuhises peab asjaomane osaleja olema märgitud makse algatajana.
(3) Internetipõhist ühendust kasutavad osalejad peavad kasutama avaliku võtme infrastruktuuri teenuseid kasutusjuhendi „Internetipõhine juurdepääs avaliku võtme sertifitseerimisteenusele" kohaselt.

2. Maksesõnumite liigid

(1) Internetipõhised osalejad võivad teostada järgmisi makseid:
a) kliendimakse, st krediidiülekanne, mille korral makse algataja ja/või makse saaja ei ole finantsasutus;
b) kliendimakse automaatseks töötlemiseks, st krediidiülekanne, mille korral makse algataja ja/või makse saaja ei ole finantsasutus ning mida töödeldakse automaatselt;
c) pankadevaheline ülekanne rahaliste vahendite ülekandmiseks finantsasutuste vahel;
d) kattemaksed (*cover payments*) rahaliste vahendite ülekandmiseks finantsasutuste vahel, mis on seotud kliendi krediidiülekannete alustehingutega.
Lisaks on maksemooduli kontole internetipõhist juurdepääsu kasutavatel osalejatel võimalik vastu võtta otsedebiteerimismakseid.
(2) Osalejad peavad järgima andmeväljade nõudeid, mis on määratletud kasutaja üksikasjaliku funktsioonikirjelduse 1. raamatu jaotises 9.1.2.2.
(3) Välja sisu kinnitatakse TARGET2-Eesti tasandil UDFSi nõuete kohaselt. Osalejad võivad omavahel väljade sisu suhtes kokku leppida erireeglites. Nende erireeglite järgimise suhtes ei teostata TARGET2-Eestis eraldi kontrolli.
(4) Internetipõhist juurdepääsu kasutavad osalejad võivad TARGET2 kaudu arveldada kattemakseid, st makseid, mida korrespondentpangad arveldavad krediidiülekande teadete alusel, mis esitatakse kliendi pangale muul otsesemal viisil. Kattemaksetes sisalduvaid kliendiandmeid ei esitata ICMis.

3. Unikaalsuse kontroll

(1) Kõik maksejuhised peavad läbima unikaalsuse kontrolli, mille eesmärk on lükata tagasi maksejuhised, mis on ekslikult sisestatud rohkem kui üks kord.

(2) Kontrollida tuleb järgmisi sõnumiliikide välju:

Selgitus	**Sõnumi osa**	**Väli**
Saatja	Põhipäis	BIC aadress
Sõnumiliik	Programmipäis	Sõnumiliik
Vastuvõtja	Programmipäis	Sihtaadress
Tehingu viitenumber (TRN)	Tekstiplokk	:20
Seotud viited	Tekstiplokk	:21
Väärtuspäev	Tekstiplokk	:32
Summa	Tekstiplokk	:32

(3) Kui uue maksejuhise kõik lõikes 2 kirjeldatud väljad on samad, mis juba vastuvõetud maksejuhises, lükatakse uus maksejuhis tagasi.

4. Veakoodid

Kui maksejuhis lükatakse tagasi, saadetakse ICMi tagasilükkamise teade, milles on tagasilükkamise põhjus näidatud veakoodiga. Veakoodid on määratletud UDFSi jaotises 9.4.2.

5. Ettemääratud arveldusajad

(1) Debiteerimise algtähtaja määranguga maksejuhistes tuleb kasutada koodi „/FROTIME/”.

(2) Debiteerimise lõpptähtaja määranguga maksejuhistes võib kasutada

a) koodi „/REJTIME/” – kui maksejuhist ei ole võimalik määratud debiteerimisajaks arveldada, tuleb maksejuhis tagasi lükata;

b) koodi „/TILTIME /” – kui maksejuhist ei ole võimalik määratud debiteerimisajaks arveldada, ei lükata maksejuhist tagasi, vaid hoitakse asjakohases järjekorras.

Mõlemal juhul, kui debiteerimise lõpptähtaja määranguga maksejuhist ei ole arveldatud 15 minutit enne selles määratud aega, postitatakse selle kohta ICMi kaudu automaatteade.

(3) Kui kasutatakse koodi „/CLSTIME/”, kohaldatakse makse suhtes sama korda nagu lõike 2 alapunktis b.

6. Maksejuhiste töötlemine sisendkontrollis

(1) Sisendkontrolli sisestatud maksejuhiste suhtes viiakse läbi tasaarvelduskontroll ning vajaduse korral laiendatud tasaarvelduskontroll (nende mõistete lõigetes 2 ja 3 esitatud määratluste kohaselt), et tagada maksejuhiste kiire ja likviidsussäästlik arveldamine.

(2) Tasaarvelduskontrolli käigus määratakse kindlaks, kas erakorraliste kiirmaksete või asjakohastel juhtudel kiirmaksete järjekorra alguses olevaid makse saaja maksejuhiseid võib tasaarveldada maksja maksejuhisega (edaspidi *tasaarveldav maksejuhis*). Kui tasaarveldav maksejuhis ei anna piisavalt vahendeid maksja maksejuhise jaoks sisendkontrollis, tuleb kontrollida, kas maksja maksemooduli kontol on piisavalt vaba likviidsust.

(3) Kui tasaarvelduskontroll ebaõnnestub, võib Eesti Pank kohaldada laiendatud tasaarvelduskontrolli. Laiendatud tasaarvelduskontrolli käigus määratakse kindlaks, kas makse saaja mis tahes järjekordades on tasaarveldavaid maksejuhiseid, olenemata nende järjekorda panemise ajast. Kui makse saaja järjekorras on kõrgema prioriteetsusega teistele TARGET2 osalejatele suunatud maksejuhiseid, võib lihtjärjekorra (*first in, first out, FIFO*) põhimõttest kõrvale kalduda ainult juhul, kui sellise tasaarveldava maksejuhise arveldamise tulemusel makse saaja likviidsus suureneb.

7. Järjekorras olevate maksejuhiste arveldamine

(1) Järjekorda pandud maksejuhiste käsitlemine sõltub neile maksealgataja poolt antud prioriteedist.
(2) Likviidsuse suurenemisel või järjekorra muutmisel (järjekoha, arveldusaja või prioriteedi muutmine või maksejuhise tühistamine) arveldatakse erakorraliste kiirmaksete ja kiirmaksete järjekorras olevad maksejuhised 6. osas kirjeldatud tasaarvelduskontrolli abil, alustades järjekorras esimesel kohal olevast maksejuhisest.
(3) Tavaliste maksete järjekorras olevad maksejuhised arveldatakse jooksvalt, lisades arveldamisse erakorralised kiirmaksejuhised ja veel arveldamata kiirmaksejuhised. Kasutatakse erinevaid optimeerimismehhanisme ehk algoritme. Kui algoritmi töö õnnestub, siis kaasatud maksejuhised arveldatakse; kui algoritmi töö ebaõnnestub, siis jäävad kaasatud maksejuhised järjekorda. Maksevoogude tasaarveldusele kohaldatakse kolme algoritmi (1–3). Algoritmi 4 kasutatakse UDFSi jaotises 2.8.1 määratletud arvelduskorra nr 5 puhul kõrvalsüsteemide maksejuhiste arveldamiseks. Kõrvalsüsteemide erakorraliste kiirtehingute arveldamise optimeerimiseks osalejate allkontodel kasutatakse erialgoritmi (algoritm 5).

a) Kõikide kahepoolse piiranguga suhete ja mitmepoolse kogusumma piiranguga suhete korral kasutab Eesti Pank algoritmi 1 (*all-or-nothing*) järgmistel eesmärkidel:
   i) iga TARGET2 osaleja maksemooduli konto üldise likviidsuspositsiooni arvutamine. Selleks tuleb tuvastada, kas kõikide järjekorras olevate väljuvate ja laekuvate maksejuhiste saldo on negatiivne või positiivne ning, kui see on negatiivne, kontrollida, kas see ületab vastava osaleja vaba likviidsust (likviidsuse saldo moodustab „kogulikviidsuspositsiooni”);
   ii) TARGET2 osaleja poolt seoses iga maksemooduli kontoga nõutud piirangute ja reserveeringute järgimise kontroll.
   Kui eelnimetatud arvutuste ja kontrollimise tulemus on kõikide asjakohaste maksemooduli kontode korral positiivne, siis Eesti Pank ja teised asjaomased keskpangad arveldavad kõik maksed ühel ajal vastavate TARGET2 osalejate maksemooduli kontodel.
b) Algoritmi 2 (*partial*) kasutab Eesti Pank järgmistel eesmärkidel:
   i) iga vastava maksemooduli konto likviidsuspositsiooni, limiitide ja reserveeringute arvutamine ja kontroll nagu algoritmi 1 puhul;
   ii) maksejuhiste ükshaaval eraldamine, kui ühe või enama vastava maksemooduli konto kogulikviidsuspositsioon on negatiivne, kuni kõikide vastavate maksemooduli kontode kogulikviidsuspositsioon on positiivne.
   Seejärel, piisavate vahendite olemasolu korral, arveldavad Eesti Pank ja teised asjaomased keskpangad kõik järelejäänud maksed (v.a eraldatud maksed) ühel ajal vastavate TARGET2 osalejate maksemooduli kontodel.
   Maksejuhiste eraldamist alustab Eesti Pank suurima negatiivse kogulikviidsuspositsiooniga TARGET2 osaleja maksemooduli kontost ning madalaima prioriteetsusega maksejuhiste järjekorra lõpust. Valik võib toimuda ainult lühikese aja jooksul, mille kestuse määrab Eesti Pank oma äranägemisel.
c) Algoritmi 3 (*multiple*) kasutab Eesti Pank järgmistel eesmärkidel:
   i) TARGET2 osalejate maksemooduli kontode paaride võrdlemine, et määrata kindlaks, kas järjekorras olevaid maksejuhiseid on võimalik arveldada nende kahe TARGET2 osaleja maksemooduli konto vaba likviidsuse ning nende kehtestatud piirangute raames (alustades väikseima arvu teineteisele adresseeritud maksejuhistega maksemooduli kontode paarist), ning asjaomased keskpangad kirjendavad need maksed ühel ajal nende kahe TARGET2 osaleja maksemooduli kontodel;
   ii) kui alajaotuses i kirjeldatud maksemooduli kontode paari likviidsus ei ole piisav kahepoolse positsiooni rahastamiseks, üksikute maksejuhiste eraldamine, kuni likviidsus on piisav. Sellisel juhul arveldavad asjaomased keskpangad järelejäänud maksed, v.a eraldatud maksed, ühel ajal nende kahe TARGET2 osaleja maksemooduli kontodel.

Pärast alajaotustes i ja ii sätestatud kontrollide teostamist kontrollib Eesti Pank mitmepoolseid arvelduspositsioone (osaleja maksemooduli konto ja teiste TARGET2 osalejate maksemooduli kontode vahel suhetes, millele on seatud mitmepoolne piirang). Sel eesmärgil kohaldatakse *mutatis mutandis* alajaotustes i–ii kirjeldatud korda.

d) Algoritmi 4 (*partial plus ancillary system settlement*) kasutab Eesti Pank selleks, et teostada sama menetlus, mis algoritmi 2 puhul, kuid eraldamata maksejuhiseid, mis on seotud arveldamisega kõrvalsüsteemis (mis arveldab samaaegsuse ja mitmepoolsuse põhimõttel).

e) Algoritmi 5 (*ancillary system settlement via sub-accounts*) kasutab Eesti Pank selleks, et teostada sama menetlus, mis algoritmi 1 korral. Erinevus on, et Eesti Pank käivitab algoritmi 5 kõrvalsüsteemiliidese kaudu ning kontrollib ainul seda, kas osalejate allkontodel on piisavalt vahendeid. Arvesse ei võeta limiite ega reserveeringuid. Algoritmi 5 kasutatakse ka öise arveldamise ajal.

(4) Pärast algoritmide 1–4 käivitamist võib sisendkontrolli sisestatud maksejuhised siiski arveldada viivitamata sisendkontrollis, kui vastavate TARGET2 osalejate maksemooduli kontode positsioonid ja piirangud võimaldavad nii nende maksejuhiste arveldamist kui ka käimasolevasse optimeerimismenetlusse kaasatud maksejuhiste arveldamist. Kahte algoritmi ei või kasutada samal ajal.

(5) Arvelduspериoodi ajal kasutatakse algoritme järjekorras. Kui samal ajal ei ole ootel kõrvalsüsteemide üheaegset mitmepoolset arveldamist, on järjekord järgmine:

a) algoritm 1;

b) kui algoritm 1 ei ole tulemuslik, siis algoritm 2;

c) kui algoritm 2 ei ole tulemuslik, siis algoritm 3, või kui algoritm 2 on tulemuslik, korrata algoritmi 1.

Kui samal ajal on ootel kõrvalsüsteemide üheaegne mitmepoolne arveldamine (arvelduskord nr 5), tuleb kasutada algoritmi 4.

(6) Algoritme tuleb kasutada paindlikult, määrates eelnevalt viivituse erinevate algoritmide kasutamise vahel, et tagada kahe algoritmi kasutamise vähim intervall. Ajalist järgnevust juhitakse automaatselt, kuid võimalik peab olema ka käsitsi sekkumine.

(7) Kui maksejuhise töötlemine algoritmiga on alanud, ei või selle asukohta järjekorras muuta ega maksejuhist tühistada. Maksejuhiste muutmise või tühistamise nõuded tuleb jätta järjekorda, kuni algoritm on lõpetanud. Kui vastav maksejuhis on algoritmi käitamise ajal arveldatud, lükatakse maksejuhise muutmise või tühistamise nõuded tagasi. Kui maksejuhist ei ole arveldatud, võetakse osaleja nõue viivitamata arvesse.

8. ICMi kasutamine

(1) ICMi võib kasutada maksejuhise sisestamiseks.

(2) ICMi võib kasutada teabe saamiseks ja likviidsuse juhtimiseks.

(3) ICMi kaudu võib saada teavet ainult jooksva päeva kohta, välja arvatud ladustatud maksejuhiseid ning staatilisi andmeid puudutav teave. Teabeaknad on ainult inglise keeles.

(4) Teavet antakse „nõudmiseni” (*pull*) režiimis, mis tähendab, et iga osaleja peab ise teavet nõudma. Osalejad kontrollivad oluliste sõnumite laekumist ICMi korrapäraselt kogu tööpäeva jooksul.

(5) Internetipõhist juurdepääsu kasutavatele osalejatele võimaldatakse ainult kasutajaltrakendusele režiimi (*user to application*, U2A). U2A võimaldab osaleja ja ICMi otsesuhtlust. Teave kuvatakse personaalarvutis töötavas veebilehitsejas. Täpsem teave on olemas ICMi kasutaja käsiraamatus.

(6) Igal osalejal peab olema vähemalt üks internetiühendusega tööjaam, et saada U2A kaudu juurdepääs ICMi.

(7) ICMi juurdepääsuõigused antakse sertifikaatidega, mille kasutamist on põhjalikumalt kirjeldatud osades 10–13.

(8) Osalejad võivad ICMi kasutada ka likviidsuse ülekandmiseks
   a) oma maksemooduli kontolt väljaspool maksemoodulit asuvale kontole;
   b) maksemooduli konto ja osaleja allkontode vahel;
   c) maksemooduli kontolt kõrvalsüsteemi hallatavale peegelduvale kontole.

9. UDFS, ICMi kasutaja käsiraamat ja kasutusjuhend „Internetipõhine juurdepääs avaliku võtme sertifitseerimisteenusele“

Lähemad üksikasjad ja näited eeltoodud reeglite kohta on UDFSis ja ICMi kasutaja käsiraamatus, mida aeg-ajalt ajakohastatakse ning mis avaldatakse Eesti Panga kodulehel ja TARGET2 kodulehel inglise keeles, ning kasutusjuhendis „Internetipõhine juurdepääs avaliku võtme sertifitseerimisteenusele” („*Internet Access for the Public Key Certification Service*”).

10. Sertifikaatide väljastamine, peatamine, taasaktiveerimine, tagasivõtmine ja uuendamine

(1) TARGET2-Eestile internetipõhise juurdepääsu saamiseks peab osaleja esitama Eesti Pangale sertifikaatide väljastamise avalduse.
(2) Kui sertifikaadi omanik ei soovi enam kasutada juurdepääsu TARGET2-le või kui osaleja lõpetab oma tegevuse TARGET2-Eestis (näiteks ühinemise või ülevõtmise tõttu), siis taotleb osaleja Eesti Pangalt sertifikaatide peatamist ja taasaktiveerimist või tagasivõtmist ja uuendamist.
(3) Osaleja võtab tarvitusele kõik ettevaatusabinõud ja meetmed, et tagada sertifikaatide kasutus kooskõlas ühtsete tingimustega.
(4) Osaleja teavitab Eesti Panka viivitamata sertifikaatide väljastamiseks Eesti Pangale esitatud vormides sisalduva teabe mis tahes olulistest muudatustest.
(5) Osalejal võib iga maksemooduli konto kohta olla maksimaalselt viis aktiivset sertifikaati. Vastava taotluse korral võib Eesti Pank omal äranägemisel taotleda sertifitseerimisasutustelt täiendavate sertifikaatide väljastamist.

11. Sertifikaatide hoidmine

(1) Osaleja peab tagama sertifikaatide turvalise hoidmise ja võtma tarvitusele ranged korralduslikud ja tehnilised meetmed, vältimaks kahju tekitamist kolmandatele isikutele, ning tagama, et sertifikaati kasutaks vaid sertifikaadi omanik.
(2) Osaleja annab viivitamata Eesti Panga nõutud teavet ning tagab selle usaldusväärsuse. Osalejad vastutavad igal hetkel täielikult Eesti Pangale sertifikaatide väljastamiseks antud teabe täpsuse eest.
(3) Osaleja vastutab täielikult selle eest, et kõik sertifikaatide omanikud hoiaksid neile väljastatud sertifikaate eraldi salastatud PIN- ja PUK-koodidest.
(4) Osaleja vastutab täielikult selle eest, et ükski sertifikaatide omanik ei kasutaks sertifikaate viisil või eesmärgil, mis ei ole kooskõlas sertifikaatide väljastamise eesmärgiga.
(5) Osaleja teavitab Eesti Panka viivitamata mis tahes sertifikaatide peatamise, taasaktiveerimise, tagasivõtmise või uuendamise taotlusest ning selle põhjustest.
(6) Osaleja esitab Eesti Pangale viivitamata taotluse defektsete või sertifikaadi omaniku valdusest väljunud sertifikaatide või neis sisalduvate võtmete peatamiseks.
(7) Osaleja teavitab Eesti Panka viivitamata sertifikaatide kaotusest või vargusest.

12. Turvanõuded

(1) Osaleja arvutisüsteem, mida ta kasutab TARGET2-le internetipõhiseks juurdepääsuks, peab asuma osaleja omandis oleval või tema poolt renditaval pinnal. Juurdepääs TARGET2-Eestile on lubatud vaid eelnimetatud pinnalt; kaugjuurdepääs on kahtluse vältimiseks keelatud.
(2) Osaleja kasutab arvutisüsteemis tarkvara, mis on installeeritud ja seadistatud kehtivate rahvusvaheliste IT-turvastandardite kohaselt, mis sisaldavad vähemalt käesoleva osa lõikes 3 ja 13. osa lõikes 4 sätestatud nõudeid. Osaleja võtab tarvitusele kõik kohased meetmed, sealhulgas

viiruse- ja pahavaratõrje, andmepüügivastased meetmed, tugevdamine (*hardening*) ja turvapaikade haldus. Osaleja ajakohastab korrapäraselt kõik eelnimetatud meetmed ja menetlused.

(3) Osaleja loob TARGET2-Eestiga internetiühenduseks krüpteeritud kommunikatsiooniühenduse.

(4) Osaleja tööjaama kasutajakontodel ei ole administraatori õigusi. Neid õigusi antakse privileegide piiratuse põhimõtte järgi.

(5) Osaleja kaitseb TARGET2-Eestiga internetiühenduseks kasutatavaid arvutisüsteeme igal hetkel järgmiselt:

a) tulemüüriga, et kaitsta arvutisüsteeme ja tööjaamu lubamatu siseneva internetiliikluse eest ning tööjaamu lubamatu juurdepääsu eest sisevõrgu kaudu. Osaleja kasutab nii siseneva liikluse eest kaitsvat tulemüüri kui ka tööjaama tulemüüri, mis tagab, et välismaailmaga suhtlevad vaid lubatud programmid;

b) osalejatel on lubatud tööjaamadesse installeerida ainult sellist tarkvara, mis on vajalik TARGET2-le juurdepääsuks ning mis on kooskõlas osaleja siseturvalisuse põhimõtetega;

c) osaleja peab igal hetkel tagama, et tööjaamades kasutatavad tarkvararakendused oleksid korrapäraselt ajakohastatud ning kasutama rakenduse kõige uuemat versiooni. See kehtib eelkõige operatsioonisüsteemi, veebilehitseja ja pistikprogrammide kohta;

d) osaleja peab igal hetkel tagama, et tööjaamast väljuv liiklus piirduks ärikriitiliste veebisaitidega ning veebisaitidega, mis on vajalikud legaalseteks ja mõistlikeks tarkvarauuendusteks;

e) osaleja peab tagama, et kõik kriitilised tööjaamadesse sisenevad ja sealt väljuvad andmevood oleksid kaitstud avalikustamise ja kuritahtliku muutmise eest, eriti kui andmefaile edastatakse võrgu kaudu.

(6) Osaleja peab tagama, et sertifikaatide omanikud järgiksid igal hetkel turvalise veebilehitsemise nõudeid, sealhulgas:

a) reserveerima teatavad tööjaamad võrdse kriitilisuse tasemega veebisaitide juurde pääsemiseks ning külastama selliseid saite ainult selliste tööjaamade kaudu;

b) alati sulgema ja taaskäivitama veebilehitseja enne ja pärast TARGET2-Eestiga interneti-ühenduse loomist;

c) kontrollima serveri SSL-sertifikaadi autentsust iga kord, kui osaleja loob interneti-ühenduse TARGET2-Eestiga;

d) olema ettevaatlik e-kirjade suhtes, mille adresseerija näib olevat TARGET2-Eesti, ning salasõna päringu korral mitte kunagi avaldama sertifikaadi salasõna, sest TARGET2-Eesti ei küsi kunagi sertifikaadi salasõna e-posti teel või muul viisil.

(7) Osaleja peab süsteemiriskide maandamiseks igal hetkel rakendama järgmisi riskijuhtimispõhimõtteid:

a) kehtestama kasutajahalduse korra, mis tagab, et juurdepääs süsteemile oleks antud ja hoitud vaid autoriseeritud kasutajatele, ning pidama täpset ja ajakohastatud nimekirja kõikidest autoriseeritud kasutajatest;

b) kooskõlastama igapäevase makseliikluse viisil, mis võimaldab tuvastada mittevastavusi lubatud ja tegeliku makseliikluse vahel nii saadetud kui ka saadud maksete korral;

c) tagama, et sertifikaadi omanik ei lehitseks TARGET2-Eestiga ühenduse ajal mõnd muud veebisaiti.

13. Täiendavad turvanõuded

(1) Osaleja peab kohaseid korralduslikke ja/või tehnilisi meetmeid tarvitusele võttes igal hetkel tagama, et juurdepääsuõiguste kontrollimiseks (*Access Right Review*) avaldatud kasutajatunnuseid ei väärkasutataks; eelkõige tagades, et need ei saaks teatavaks mittevolitatud isikutele.

(2) Osaleja kehtestab kasutajahalduse korra, tagamaks kasutajatunnuse viivitamatu ja lõpliku kustutamise juhul, kui mõni töötaja või muu osaleja pinnal arvutisüsteemi kasutaja lahkub osaleja organisatsioonist.

(3) Osaleja kehtestab kasutajahalduse korra ning blokeerib viivitamata ja lõplikult kõik kasutaja-tunnused, mille turvalisus on ühel või teisel viisil ohustatud, k.a sertifikaatide kaotuse või varguse ning juhtumite korral, kus salasõna on tuvastatud andmepüügi teel.
(4) Kui osaleja ei suuda parandada turva- või seadistusvigu (näiteks vead pahavaraga nakatunud süsteemis) pärast kolme intsidenti, võib ühisplatvormi käitav keskpank lõplikult blokeerida kõik asjaomase osaleja kasutajatunnused.

IIA liide

Internetipõhise juurdepääsu tasud ja arved

Otseosalejate tasud

1. Otseosalejate maksejuhiste töötlemise kuutasu TARGET2-Eestis on 70 eurot iga internetipõhise juurdepääsu eest maksemooduli kontole, millele lisandub 100 eurot iga maksemooduli konto eest, ning 0.80 eurot iga tehingu eest (deebetkanne);
2. Otseosalejad, kes ei soovi oma konto BIC koodi TARGET2 kataloogis avaldada, tasuvad lisatasu 30 eurot kuus konto kohta.

Arved

3. Otseosalejate suhtes kehtivad järgmised arvete esitamise reeglid. Otseosaleja saab eelmise kuu arve, millel on ära näidatud maksmisele kuuluvad tasud hiljemalt järgmise kuu viiendaks tööpäevaks. Arve tuleb tasuda hiljemalt kuu kümnendaks tööpäevaks Eesti Panga osutatud kontole ja see debiteeritakse selle osaleja maksemooduli kontolt.