RAHANDUSMINISTEERIUM

E-residentidele pangakontode avamise hõlbustamise võimaluste analüüs

Tallinn 2015

Sisukord

1 Sissejuhatus 3
2 Analüüsi eesmärk 3
3 Analüüsi struktuur 3
4 Analüüsi põhijärelduste kokkuvõte 4
5 Kontosuhte regulatsioon 5
5.1. Rahvusvahelised nõuded 5
5.2. Siseriiklikud nõuded 5
6 Näost näkku tuvastamise nõue, selle eesmärgid ja erandid 6
6.1. Näost näkku tuvastamise kohustus 6
6.2. Näost näkku tuvastamise kohustuse eesmärgid 6
6.3. Näost näkku tuvastamise erandid 8
6.4. Näost näkku tuvastamise nõude kehtestamise alused 8
7 Näost näkku tuvastamise nõude kaotamisega seotud riskide ja võimalike mõjude analüüs 9
7.1. E-residendi digitaalse isikutunnistuse mõju- ja riskianalüüsi puudumine 9
7.2. Eesti rahapesu ja terrorismi rahastamise riskid 10
7.3. Mitteresidentide arvu suurenemisega seotud riskid 10
7.4. Menetlus-, kriminaal- ja haldusõiguslikud ning põhiseaduslikud probleemid 11
7.5. Terrorismi leviku suurenemise risk 12
7.6. Eesti rahvusvahelise standardi languse ja teiste riikidega suhete halvenemise risk 12
7.7. Halduskoormuse tõus ja sellega seotud mõjud 13
7.8. Kaugkanalite kaudu loodud õigussuhete kehtima jäämisega seonduvad riskid 13
7.9. eIDAS rakendusaktide puudumisega seonduvad riskid 13
7.10. Pangakontode registri ja asjakohaste arstimis- ning konfiskeerimismeetmete puudumisega seotud riskid 14
7.11. Krediidi väljastamisega seotud riskid 14
7.12. Eesti välisesinduste töökoormuse ja põhifunktsioonide muutumisega seotud riskid 14
8 E-residentidele pangakonto avamise hõlbustamise võimalused: järeldused ja ettepanekud 15

1 Sissejuhatus

Valitsuskabinet andis 2014. a. lõpus Rahandusministeeriumile ülesande analüüsida koostöös Majandus- ja Kommunikatsiooniministeeriumiga võimalusi e-residentidele pangakontode avamise hõlbustamiseks.[1] Käesolev analüüsi on koostatud valitsuskabineti ülesande täitmiseks Rahandusministeeriumi ettevõtluse ja arvestuspoliitika osakonna jurist Veronika Mets (611 3169, veronika.mets@fin.ee). Analüüsi koostamisel andis panuse finantsturgude osakonna peaspetsialist Kadri Siibak (611 3718, kadri.siibak@fin.ee). Lisaks kogus Rahandusministeerium analüüsi koostamiseks arvamusi asjakohastelt asutustelt ning sise- ja välisekspertidelt.[2]

2 Analüüsi eesmärk

Käesoleva analüüsi eesmärk on analüüsida e-residentidele[3] pangakontode avamise hõlbustamise võimalusi rahapesu ja terrorismi rahastamise tõkestamise seaduses (edaspidi *RahaPTS*)[4] sätestatu raames.

3 Analüüsi struktuur

Käesoleva analüüsi alguses on toodud analüüsi põhijärelduste kokkuvõte, millele järgneb täpsem analüüs. Analüüs algab kontosuhte nõuete kirjeldamisega. Selgitatud on RahaPTS § 15 lõikes 1 nimetatud isiku samas kohas viibides isikusamasuse tuvastamise (edaspidi *näost näkku tuvastamine*) eesmärke ja nimetatud nõude suhtes kehtivaid erandeid. Järgmisena on analüüsitud näost näkku tuvastamise nõude muutmisega seonduvaid riske ja mõjusid ning e-residentidele konto avamise hõlbustamise võimalusi. Analüüs lõpeb järelduste ja ettepanekute esitamisega.

---

[1] 2014. aasta 22. aprilli valitsuskabineti nõupidamisel kiideti heaks kontseptsioon mitteresidentidele Eesti digitaalse isikutunnistuse väljastamiseks ehk e-residentsuse käivitamiseks. Selle alusel töötati välja isikut tõendavate dokumentide seaduse (edaspidi *ITDS*) muudatused, millele Rahandusministeerium esitas märkused ja ettepanekud 20. mai 2014. a. kirjaga nr 12.2-4/05840-1 ja 25. juuni 2014. a. kirjaga nr 1.1-11/05840-5. Siseministeerium eelnõu väljatöötajana Rahandusministeeriumi märkuste ega ettepanekutega eelnõu menetluse käigus sisuliselt ei arvestanud. Eelnõu võttis Riigikogu vastu 21.oktoobril 2014. a. ja see jõustus 1.detsembril 2014. a.

[2] Oma sisendi andsid Finantsinspektsioon, Välisministeerium, Justiitsministeerium, prokuratuur, Siseministeerium, Politsei- ja Piirivalveamet, Rahapesu andmebüroo, Kaitsepolitseiamet ja Eesti Pangaliit. Täiendavalt on analüüsitavat teemat arutatud Eesti Pangaliidu liikmetega, Majandus- ja Kommunikatsiooniministeeriumi moodustatud e-residentsuse nõukojas ja rahapesu ja terrorismi rahastamise tõkestamise turuosaliste nõukojas. Lisaks on Rahandusministeerium palunud ekspertarvamusi IMF-i ja Maailmapanga ekspertidelt ning vandeadvokaat Marko Kairjakilt.

[3] E-residentsust on võimalik taotleda kõigil välismaalastel, kes soovivad Eesti e-teenuseid kasutada, ja seda nii eraisikutele kui ka ettevõtetele. **Aastaks 2025 on maailmas oodatavalt kokku 10 miljonit e-eestlast ehk e-residenti.** E-residentsus annab välisriikides elavatele välismaalastele Eesti elanikega sarnased võimalused Eesti e-keskkonnas tegutsemiseks, sh allkirjastada dokumente ja kasutada erinevaid teenuseid, elades ise mujal. Täpsem info Majandus ja Kommunikatsiooni ministeeriumi kodulehel: https://www.mkm.ee/et/eesti-alustas-e-residentsuse-programmiga.

[4] Rahapesu ja terrorismi rahastamise tõkestamise seadus, RT I, 19.03.2015, 54, https://www.riigiteataja.ee/akt/119032015054

Käesolevale analüüsil on järgmised lisad:
lisa 1 „Kontosuhte regulatsioon“, 11 lk;
lisa 2 „Andmete kogumine ja säilitamine“, 3 lk;
lisa 3 „Rahvusvaheliste nõuete järgimise kohustus ja rahvusvahelised arengud“, 4 lk;
lisa 4 „Näost näkku tuvastamise nõude erandid RahaPTS-is“, 3 lk;
lisa 5 „Näited teiste riikide seadusandlustest ja praktikast“, 5 lk;

4 Analüüsi põhijärelduste kokkuvõte[5]

E-residentidele pangakontode avamise hõlbustamiseks saab kehtestada RahaPTS § 15 lõikes 1 toodud näost näkku tuvastamise nõudele asjakohase erandi, mis sätestab järgmised hoolsusmeetmed võimalike kuritarvituste ennetamiseks:

E-residentidele, keda pole näost näkku tuvastatud, tuleks konto avada üksnes juhul, kui:[6]

1) isikul on mõjuv põhjus Eestis konto avamiseks, sh selgitatakse välja tehingute eesmärk;[7]
2) isikusamasuse kontrollimiseks kasutatakse infotehnoloogilisi vahendeid, mille pildi- ja helikvaliteet võimaldab kontot avada sooviva isikuga suhelda vahetult, võrrelda tema nägu esitatud isikut tõendava dokumendil oleva pildiga, kontrollida e-residentsuse kaardi olemasolu ja viia läbi muud toimingud isiku tausta, rahaliste vahendite päritolu ning tehingu eesmärgi kontrollimiseks (nn tunne-oma-klienti-printsiibi täitmine);
3) punktis 2) toimingud tuleb salvestada;[8]
4) avatavale kontole tehakse esimene makse samale isikule kuuluva konto kaudu, mis on avatud krediidiasutuses, kellel on tegevuskoht Euroopa Majanduspiirkonna lepinguriigis või riigis, kus kehtivad RahaPTS-iga võrdväärsed nõuded;
5) kontole kantavate rahaliste vahendite päritolu kontrollitakse ja jälgitakse tugevdatud korras ning nimetatud nõuded täpsustatakse rahandusministri määruses;[9]
6) e-residendist füüsilise isiku ja e-residendi poolt registreeritud juriidilise isiku isikusamasuse tuvastab, vastavad andmed kogub ja säilitab krediidiasutus RahaPTS-i 2. jaos toodud korras. Täiendavalt kogutakse ja säilitatakse e-residendi isikut tõendava dokumendi koopia, mille isikuandmete ja fotoga leheküljest tehakse koopia.[10]

[5] Täpsemalt vt punkt VIII „Järeldused ja ettepanekud“.
[6] Lisaks nimetatud lisameetmetele tuleb rakendada ka RahaPTS-is toodud muid hoolsusmeetmeid, sh nt andmete säilitamise kohustus jne.
[7] Vastavaid täiendavaid selgitusi küsib ja kontrollib konto avamisel pank.
[8] Perioodi täpne pikkus on kaalumisel, kuid tõenäoliselt on perioodiks mitte vähem kui 6 kuud. Pangaliiduga on antud ettepanekut arutatud.
[9] Koostöös Pangaliidu ja asjakohaste asutustega tuleks kaaluda näiteks summaliste ja sularaha väljavõtmisega seotud piirangute kehtestamist.
[10] E-residendi kaart ei ole isikut tõendav ega reisidokument ning sellel puudub isiku pilt. Hetkel saaks X-tee päringuga väljastama pankadele Politsei- ja Piirivalveameti infosüsteemi kogutud andmeid dokumendi kohta

5 Kontosuhte regulatsioon

5.1. Rahvusvahelised nõuded

Erinevates rahvusvahelistest konventsioonidest, standarditest, soovitustest ja Euroopa Liidu õigusaktidest tulenevad pangakontode avamist, ligipääsu ja kasutamist reguleerivad nõuded, mis on seotud oluliste õigushüvede kaitsega, pannes krediidiasutustele erinevaid avalik-õiguslikke kohustusi. Krediidiasutustel on võimalik neid ülesandeid tõhusalt täita vaid juhul, kui seadusandjad annavad krediidiasutustele õigusliku võimaluse saada võimalikult täpset teavet kliendi isiku identiteedi, tema isikuandmete, majandusliku seotuse ja tehingute eesmärkide kohta. Täpsemalt on kontosuhte rahvusvahelisi nõudeid kirjeldatud lisas 1.

5.2. Siseriiklikud nõuded

5.2.1. Hoolsusmeetmete rakendamine

Rahapesu ja terrorismi rahastamise oht on alati olnud suurim finantssektoris, mistõttu on Financial Action Task Force (edaspidi *FATF*)[11] kehtestanud finantsteenuste osutajatele eraldi hoolsusmeetmed (edaspidi *FATF-i soovitused*), mis on Euroopa Liidu tasandil üle võetud Euroopa Parlamendi ja nõukogu rahapesu ja terrorismi rahastamise tõkestamise direktiiviga 2005/60/EÜ (edaspidi *III rahapesu tõkestamise direktiiv*)[12] ja III rahapesu tõkestamise direktiivi rakendamiseks antud direktiiviga 2006/70/EÜ rakendusmeetmete kehtestamise kohta (edaspidi *rakendusdirektiiv*).[13] 2012. a. avaldatud FATF-i uute soovituste ülevõtmiseks ning rahapesu ja terrorismi rahastamise tõkestamise meetmete tõhustamiseks Euroopa Liidus töötas Euroopa Komisjon välja uue rahapesu ja terrorismi rahastamise tõkestamise alase direktiivi (edaspidi *IV rahapesu tõkestamise direktiiv*),[14] mille Euroopa Parlament kinnitas 2015. a. mais (jõustub 2015. aasta 26. juunil).[15] Nimetatud nõudeid on siseriiklikult üle võetud RahaPTS-i ja krediidiasutuste seadusega (edaspidi *KAS*).[16]

(liik, nr, kehtivusaeg, väljaandja), mille alusel väljastatakse e-residendile digi-ID. Kaaluda võiks infosüsteemide arendamist selliselt, et kõik digi-ID menetluse raames kogutud dokumendid oleks skänneeritud Politsei- ja Piirivalveameti infosüsteemi, et neid X-tee päringuga väljastada ka pankadele.

[11] Financial Action Task Force (FATF) on OECD alla kuuluv valitsustevaheline organ, mille peamisteks ülesanneteks on töötada välja rahvusvahelisi rahapesu ja terrorismi leviku ning rahastamise tõkestamise alaseid standardeid ning oma liikmesriikide hindamine antud standardite täitmise osas. Täpsemalt: http://www.fatf-gafi.org/ ja http://www.oecd.org/cleangovbiz/toolkit/moneylaundering.htm

[12] Euroopa Parlamendi ja nõukogu 26. oktoobri 2005. a. direktiiv 2005/60/EÜ rahandussüsteemi rahapesu ja terrorismi rahastamise eesmärgil kasutamise vältimise kohta, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:et:PDF

[13] Komisjoni direktiiv 2006/70/EÜ, 1. august 2006 , Euroopa Parlamendi ja nõukogu direktiivi 2005/60/EÜ rakendusmeetmete kehtestamise kohta seoses mõistega riikliku taustaga isik ning kliendi suhtes lihtsustatud nõuetekohaste hoolsuse menetluste ja harva või väga piiratud mahus teostatud finantstegevuse alusel tehtud erandite tehniliste kriteeriumide kohta *ELT L 214, 4.8.2006, lk 29—34,* http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32006L0070&rid=2

[14] IV rahapesu ja terrorismi finantseerimise tõkestamise alane direktiivi ettepaneku versioon: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0045

[15] Direktiiv jõustub 20 päeva jooksul arvates selle avaldamisest Euroopa Liidu Teatajas, kuid direktiivis sätestatud meetmed tuleb liikmesriikidel üle võtta kahe aasta jooksul arvates selle jõustumisest. IV rahapesu

5.2.2. Andmete kogumine ja säilitamine

Konto avamisel tuleb isik tuvastada, koguda asjakohased andmed ja dokumendid ning need säilitada vastavalt RahaPTS 2. peatüki 2. jaos sätestatud korrale. Nimetatud meetmed tulenevad FATF-i soovitustest ja III rahapesu tõkestamise direktiivist.[17] Teatud tingimustel on lubatud ärisuhte loomisel tugineda teise isiku teostatud hoolsusmeetmete kohaldamise tulemusele, kuid lõplik vastutus kliendi suhtes rakendatava nõuetekohase hoolsuse menetluse osas on alati krediidi- või finantseerimisasutusel, kes sõlmib ärisuhte isikuga. Täpsemalt on andmete kogumise ja säilitamise nõudeid kirjeldatud lisas 2 „Andmete kogumine ja säilitamine“.

5.3. Rahvusvaheliste nõuete järgimise kohustus, mõju Eesti Vabariigi mainele ja rahvusvahelised arengud

Eesti rahvusvaheline maine sõltub rahvusvaheliste nõuete korrektsest täitmisest. Võttes rahvusvahelisi kohustusi, sealhulgas näiteks liitudes rahvusvahelise organisatsiooni, komitee või konventsiooniga, tuleb võetuid kohustusi riigil täita, see mõjutab otseselt Eesti Vabariigi mainet ja riigile antavaid hinnanguid. Täpsemalt on rahvusvaheliste nõuete järgimise kohustust, mõju Eesti Vabariigi mainele ja rahvusvahelisi arenguid kirjeldatud lisas 3 „Rahvusvaheliste nõuete järgimine, mõju Eesti Vabariigi mainele ning rahvusvahelised arengud“.

6 Näost näkku tuvastamise nõue, selle eesmärgid ja erandid

6.1. Näost näkku tuvastamise kohustus

RahaPTS § 15 lõige 1 sätestab kohustuse tuvastada isik konto avamisel näost näkku järgmiselt: *Krediidiasutuses või finantseerimisasutuses konto avamisel või muu teenuse esmakordsel kasutamisel isiku poolt, kellega krediidiasutusel või finantseerimisasutusel ei ole ärisuhet, tuleb tehingus osaleva või teenust kasutava isiku isikusamasus tuvastada, viibides isiku või tema esindajaga samas kohas.*

Lisaks on RahaPTS § 15 lõike 2 kohaselt krediidi- ja finantseerimisasutustel keelatud osutada teenuseid, mida on võimalik kasutada ilma tehingus osaleva isiku isikusamasust tuvastamata ja esitatud teavet kontrollimata.

6.2. Näost näkku tuvastamise kohustuse eesmärgid

RahaPTS § 15 lõikes 1 sätestatud näost näkku tuvastamisel on mitu olulist eesmärki:

---

tõkestamise direktiiv avaldati Euroopa Liidu Teatajas 05. juunil 2015. a., direktiiv jõustub 26. juunil 2015. a. ja ülevõtmise tähtaeg on 26. juuni 2017. a.

[16] Krediidiasutuste seadus, RT I, 19.03.2015, 41, https://www.riigiteataja.ee/akt/119032015041

[17] Riikidel on lisaks õigus vajadusel kehtestada FATF-i soovitustes ja III/IV direktiivis sätestatud nõuetest rangemaid nõudeid.

6.2.1. Isiku tuvastamine

RahaPTS seletuskirja kohaselt on § 15 lõikes 1 sätestatud näost näkku tuvastamise nõude eesmärk vältida sidevahendite kaudu ärisuhte loomisel, sh sidevahendi kaudu konto avamisel lepingu sõlmimisega kaasnevaid kõrgendatud riske, sealhulgas riske, mis kaasnevad uute tehnoloogiate kasutamisega finantsteenuste osutamisel. Sellisteks riskideks on näiteks variisikute kasutamine ja identiteedi vargused.[18] Näost näkku tuvastamise nõue on seadusesse sisse toodud praktilisest vajadusest tõkestada variisikute ja varifirmade kasutamist ning vähendada täiendavate hoolsusmeetmete kohaldamisega seotud halduskoormust ning sellega seotud kulusid. **Pangandussektorit peetakse klassikaliselt üheks olulisemaks lüliks rahapesu skeemides.**

6.2.2. Kliendiprofiili kindlaksmääramine, sh tunne oma klienti põhimõtte rakendamine

Lisaks isikusamasuse tuvastamisele on finantsteenuse osutamise tingimuseks ka kliendi riskiprofiili, sh tahteavalduste, tegelike vajaduste, võimaluste ja riskitaluvuse kindlaksmääramine. Isikusamasuse tuvastamine on ärisuhte loomise eeldus, kuid see ei ole ainuke tingimus tehingu tegemiseks. Kliendi riskiprofiili on võimalik paremini määrata, kui ärisuhte loomine toimub vahetus kontaktis. Teenuse pakkuja peab saama üldjuhul eelnevalt veenduda, et pakutav teenus rahuldab kliendi tegelikke eesmärke ja et ei kahjustata krediidi- või finantseerimisasutuse enda ja tema teiste klientide huve.[19]

Lisaks on kohustatud isikul kohustus tuvastada ärisuhte loomisel ja tehingute tegemisel (sh pangakonto avamisel) ärisuhte ja tehingu eesmärk.[20] **Ärisuhte ja tehingu eesmärgi kohta teabe hindamisel tuleb arvestada tunne-oma-klienti-põhimõtet**. Tunne-oma-klienti-põhimõttel on laialdasem tähendus ja see ei piirdu ainuüksi rahapesu ja terrorikuritegude rahastamise tõkestamise aspektidega. Eelnimetatud põhimõtet rakendatakse usaldussuhtel põhinevate teenuste osutamisel, eeskätt finantsteenuste osutamisel, kui teenuseosutaja hoolsuskohustuse ulatus, eelkõige teabe andmise kohustuse ulatus, sõltub kliendi teadlikkusest teenuse eesmärkidest ja teenusega kaasnevatest riskidest ning muudest asjaoludest, mis puudutavad finantsturu toimimist üldisemalt. Tunne-oma-klienti-põhimõte on kõige olulisem vahend kliendi või tehingu teise poole isiku ja tema tegevusega kaasnevate ohtude ärahoidmiseks ja kohustatud isiku enda tegevusriskide hindamiseks. Kohustatud isik peab teadma, kellega ta teeb tehingu, kes osaleb ametitoimingus või kes on tema kliendiks ja milline on selle isiku tavapärane tegevus. Kohustatud isik peab jälgima, et tehingud mida klient teeb, ja tema kasutatavad rahalised vahendid oleksid kooskõlas kliendi majandustegevuse laadi ja ulatusega. Just tunne-oma-klienti-põhimõtte rakendamine annab

[18] Täpsemalt vaata rahapesu ja terrorismi rahastamise tõkestamise seaduse seletuskirjas toodud selgitusi paragrahvile 15, seletuskiri kättesaadav: http://www.riigikogu.ee/?page=eelnou&op=ems2&emshelp=true&eid=163492&u=20150407132908

[19] Täpsemalt vaata Rahapesu ja terrorismi rahastamise tõkestamise seaduse seletuskirjas toodud selgitusi §-le 15, seletuskiri kättesaadav: http://www.riigikogu.ee/?page=eelnou&op=ems2&emshelp=true&eid=163492&u=20150407132908

[20] Antud nõue tuleneb rahvusvahelistest nõuetes mida on kirjeldatud punktis 4.1.

võimaluse ära tunda tehingud, mis võivad olla seotud rahapesu või terrorikuritegude rahastamisega.[21]

Üldjuhul eelistavad krediidi- ja finantseerimisasutused kohtuda ärisuhte loomisel kontot avada sooviva isikuga, viibides temaga samas kohas, et läbi viia vastav asjakohane intervjuu, et koos isikusamasuse tuvastamisega tuvastada kliendiprofiil ja täpsustada kliendi isikuandmeid, mis ei pruugi olla üheselt leitavad elektroonilistest andmebaasidest (näiteks telefoninumbrid, andmed ärisuhte olemuse ja eesmärgi kohta jmt).

Sellist praktikat järgitakse laialdaselt ka riikides, kus isiku näost näkku tuvastamine ei tulene otseselt seadusest. Vastav praktika kehtib enamikus Euroopa Liidu riikides. Samamoodi kui Eestis kehtib seaduse tasandil isiku näost näkku tuvastamise nõue esmase ärisuhte loomisel ka mitmes teises riigis. Näiteks kehtib sama põhimõte Tšehhis, Sloveenias, Horvaatias ja Ungaris, millele kehtivad nagu Eestiski teatavad erandid. Riigid, kes ei ole kehtestanud näost näkku tuvastamise nõuet pangakonto avamisel, on kehtestanud erinevaid täiendavaid hoolsusmeetmeid vahetu kontaktita loodud ärisuhte loomiseks.[22] Tulenevalt FATF-i soovitustest on vahetu kontaktita[23] loodud ärisuhe või tehing kõrgema rahapesu ja terrorismi rahastamise riskiga, mistõttu on hoolsusmeetmete kohaldamine tugevdatud korras kohustuslik ja riskide realiseerumise ärahoidmiseks tuleb täiendavaid meetmeid vajadusel kehtestada seaduse tasandil. Distantsil loodud ärisuhte ja/või pangakonto avamisel täiendavate hoolsusmeetmete ehk hoolsusmeetmete tugevdatud korras kohaldamise vajadust on kinnitanud ka näiteks IMF ja Maailmapanga finantseksperdid.[24]

6.3. Näost näkku tuvastamise erandid

Juba praegu sisaldab RahaPTS erinevaid erandeid RahaPTS § 15 lõikes 1 sätestatud näost näkku tuvastamise nõudele, sealhulgas töötati RahaPTS § 15 lõigetes 4^2 ja 4^3 sätestatud erandid välja alles mõned aastad tagasi koostöös Eesti Pangaliiduga ja need jõustusid 2012. aasta 18. mail. RahaPTS § 15 lõikele 1 kehtivaid erandeid on kirjeldatud täpsemalt lisas 4 „Näost näkku tuvastamise nõude erandid RahaPTS-is“.

6.4. Näost näkku tuvastamise nõude kehtestamise alused

<u>Riskipõhise lähenemise rakendamise kohustus</u>

[21] Täpsemalt vaata Rahapesu ja terrorismi rahastamise tõkestamise seaduse seletuskirjas toodud selgitusi §-le 15, seletuskiri kättesaadav:
http://www.riigikogu.ee/?page=eelnou&op=ems2&emshelp=true&eid=163492&u=20150407132908
[22] Täpsemalt lisas 5 „Näited teiste riikide seadusandlustest ja praktikast“.
[23] Vahetuks kontaktiks loetakse isikuga samas kohas viibimist.
[24] IMF-i 29.04.2015.a. kiri Rahandusministeeriumile.
[24] Maailmapanga finantseksperdi 14.05.2015.a. kiri Rahandusministeeriumile

Näost näkku tuvastamise nõude kohaldamist seaduse tasandil ei sätesta otseselt FATF-i soovitused, III ega IV rahapesu tõkestamise direktiiv. Samas tuleneb FATF-i soovitustest (FATF-i soovitus nr 1) ning III ja IV rahapesu tõkestamise direktiivist riikide kohustus tuvastada ja hinnata oma rahapesu ja terrorismi rahastamise riske ning kehtestada vastavad rahapesu ja terrorismi rahastamise tõkestamise meetmed, sh vajadusel rangemad kui on ette nähtud FATF-i soovitustes ning III ja IV rahapesu tõkestamise direktiivis.[25] Kuna riikide rahapesu ja terrorismi rahastamise riskid on väga erinevad,[26] siis võivad erineda ka rakendatavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks.[27]

RahaPTS § 15 lõikes 1 sätestatud näost näkku tuvastamise nõuet ja selle suhtes kehtivaid erandeid on analüüsinud MONEYVAL-i eksperdid aastatel 2013 - 2014 läbiviidud MONEYVAL-i IV hindamisvooru raames. MONEYVAL-i eksperdid hindasid nimetatud nõuet kõrgelt, kuna see aitab rahvusvaheliste ekspertide hinnangul maandada uute tehnoloogiate kasutamisega seonduvaid riske.[28] Vastava FATF-i soovituse hindeks anti „nõuetele vastav“[29] ja MONEYVAL-i eksperdid ei soovitanud näost näkku nõude muutmist.[30]

7 Näost näkku tuvastamise nõude kaotamisega seotud riskide ja võimalike mõjude analüüs

7.1. E-residendi digitaalse isikutunnistuse mõju- ja riskianalüüsi puudumine

Üheks kriitiliseks probleemiks on e-residentsuse programmi mõjude hindamise ja riskianalüüsi puudumine. Nimetatud puudusele on viidanud enamik arvamusi esitanud asutusi. Majandus- ja Kommunikatsiooniministeeriumil, kui e-residentsuse programmi peavastutajal tuleb koostada põhjalik mõju- ja riskianalüüs ning kaasata selle koostamisse kõik programmiga seotud osapooled. Hetkel jääb selgusetuks riigi tehtavate investeeringute ning planeeritava tulu proportsioon, sh kulude ja tulude jagunemine era- ja avaliku sektori vahel. Ei ole selge, kas, kuidas ja mis ulatuses katavad programmi tulud riigi tehtud kulutusi. Juhul, kui programmi kulud ongi planeeritud ületama tulusid, on vajalik kaudsete tulude (nt mainekujundus) selgem kirjeldamine. Majandus- ja Kommunikatsiooniministeeriumil tuleks koostada prognoos programmiga seotud otsestest ja kaudsetest kuludest ning täpsustada e-residentide maksustamisest, riigilõivust ja e-teenuste tarbimisest planeeritud tuludest. Rahandusministeeriumile esitatud arvamused sisaldasid mitmeid ettepanekuid riskide ja mõjude analüüsi läbiviimiseks, mida tuleks vastavate analüüside koostamisel arvestada.

[25] III ja IV rahapesu tõkestamise direktiivid on miinimumharmoniseerimist nõudvad direktiivid.
[26] Rahapesu ja terrorismi rahastamise riksid sõltuvad väga paljudest erinevatest faktorites, nagu näiteks üldisest maksu- ja kriminaalpoliitikast, haldusvõimekusest, korruptsiooni tasemest, geograafilisest asetusest (mõjud naabberiikidest) jne.
[27] Nimetatud lähenemist nimetatakse riskipõhiseks lähenemiseks (ingise k. *risk based approach*).
[28] Nendeks on riskid, mis on seotud vahetu kontaktita ärisuhte loomisega.
[29] Inglise k. *compliant* (lühend: C)
[30] Eesti IV hindamisvooru raport, lk 128-131:
http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/MONEYVAL(2014)20_Estonia.pdf

7.2. Eesti rahapesu ja terrorismi rahastamise riskid

Eesti rahapesu ja terrorismi rahastamise riskihinnang (edaspidi *riskihinnang*)[31] näitas, et enim levinud eelkuritegu rahapesu menetlustes aastatel 2010 - 2013 oli arvutikelmus. Jätkuvalt on murekohaks suured idasuunalised sularahavood, mis läbivad Eesti finantssüsteemi.[32] Pangandussektoris tuvastati peamisteks rahapesualasteks riskiteguriteks:

- **mitteresidendist klientide hoiuste suhteliselt suur osakaal, eriti üksikute krediidiasutuste puhul**;
- mitteresidentide hoiuste koondumine üksikute ülisuurte jääkidega klientide kätte;
- keerukate omandistruktuuride puhul on keeruline tuvastada tegelikku kasusaajat.

Näost näkku tuvastamise nõude (RahaPTS § 15 lg 1) muutmise vajadust riskihinnangu käigus ei tuvastatud.[33]

7.3. Mitteresidentide arvu suurenemisega seotud riskid

E-residentsuse projekti üks eesmärk on võimaldada mitteresidentidel lihtsat ligipääsu e-teenustele, sh registreerida äriühing ja avada konto isikutele, kelle tegevusel ei pruugi olla majanduslikku seosest Eestiga. Kolmandate riikide klientide arvu suurenemisega krediidi- ja finantseerimisasutustes tõusevad oluliselt rahapesu ja terrorismi rahastamise riskid, likviidsus- ja operatsiooniriskid ning *offshore* riigi maine omandamise risk.

7.3.1. Mitteresidentide arvu suurenemisega seotud rahapesu ja terrorismi rahastamise riskid

Rahandusministeeriumi, Siseministeeriumi ja Finantsinspektsiooni hinnangul võib seniste nõuete lihtsustamine suurendada kuritegude toimepanekut Eesti kaudu, mistõttu suurenevad julgeoleku, rahapesu ja terrorismi rahastamise riskid. Väärkasutuse juhtumite ja kuritegevuse kasvu ning nende võimaliku negatiivse mõju pankade ja riigi mainele ning halduskoormusele on välja toonud ka Eesti Pangaliit ja Justiitsministeerium.

7.3.2. Kolmandate riikide klientide arvu suurenemisega seotud likviidsus- ja operatsiooniriskid

Klientide distantsilt isikutuvastamisele põhinev ärimudel seab krediidiasutusele oluliselt suurema väljakutse tuvastada rahapesu ja terrorismi tõkestamise eesmärgil asjaolusid. **Kolmandate riikide klientide arvu suurenemisel finantsasutustes (eelkõige pankades) võib olla nii likviidsus- kui ka operatsiooniriskile suurendav mõju. Samuti tuleb siin silmas pidada, et võimaliku maksejõuetuse korral kannab hoiuste tagamise riski Eesti**

[31] Riskihinnang kinnitati rahapesu ja terrorismi rahastamise valitsuskomisjoni poolt 05.01.2015.a. Riskihinnangu koostamisel osalesid kõik asjakohased ministeeriumid ja asutused, samuti erasektori esindajad. Riskihinnangu koostati vastava Maailmapanga metoodika alusel ja juhendamisel.

[32] Tulenevalt Eesti geograafilisest asetusest, vene keele oskuse kõrgest tasmest jne on Eesti atraktiivne transiitriik ida suunalistele mustadele raha voogudele.

[33] Riskihinnangu koostamisse olid kaasatud ka kohustatud subjektide esindajad, sh Eesti Pangaliit. Lisaks tuleb silmas pidada, et kohustatud subjektide jaoks vajalikud uued erandid RahaPTS-is (RahaPTS § 15 lg 4^2 ja 4^3) töötati välja koostöös Eesti Pangaliiduga alles mõned aastad tagasi ja need jõustusid 18.05.2012.a.

hoiuste tagamise fond, sõltumata kliendi residentsusest. **Operatsiooniriski**[34] **realiseerumine rahapesu valdkonnas võib pangasektoris kaasa tuua tagajärjed finantssektori usaldusväärsusele (sh tõrked teiste pankadega rahvusvahelistes korrespondentsuhetes ja reputatsioonirisk); konkreetse krediidiasutuse puhul võib operatsiooniriski realiseerumine väljenduda ka kõrgemas kapitalinõudes (SREP**[35] **hinnangute kaudu).** Täpsemalt on kolmandate riikide klientide arvu suurenemisega seotud likviidsus- ja operatsiooniriske kirjeldanud Finantsinspektsioon Rahandusministeeriumile esitatud arvamuses.

7.3.3. *Offshore*-riigi maine omandamise risk

E-residentsuse projekti raames soovitakse soodustada kaugjuhitavate äriühingute teket Eestis. Juhul, kui seos Eestiga ei ole kaugjuhitava äriühingu puhul edaspidi oluline, oleks praktikas pea võimatu ennetada seda, et Eesti ei muutu *offshore*-riigiks. Praktika on näidanud, et selline poliitika kätkeb endas mitmeid olulisi haavatavusi riigile.

7.4. Menetlus-, kriminaal- ja haldusõiguslikud ning põhiseaduslikud probleemid

7.4.1. Menetlusõiguslikud probleemid

Seoses e-residentsusega võib suureneda oht kuritegude toimepanemiseks ning raskemaks minna rahapesu süüdlaste tuvastamine ja vastutusele võtmine. E-residentide puhul on tegemist välisriikide kodanikega, kellega suhtlemine toimub õigusabitaotluste kaudu. Sellega seoses hakkab menetlusaeg rahapesu kriminaalasjades venima ja kahtlaste pangaülekannete uurimine ei ole enam nii operatiivne ja efektiivne. Lisaks saab väga keeruline olema tuvastada, kes reaalselt e-residendi identiteeti kasutas - kas isik ise või keegi teine.[36] Raske on prognoosida kui tõsiseks probleemiks võib võõra identiteedi kasutamine kujuneda. Kuna tegemist on välisriikide kodanikega, siis reaalse kasutaja tuvastamine, mis leidis aset välisriigis, ei ole Eesti õiguskaitseorganite poolt võimalik ja ei ole usutav, et välisriigid selles osas olulist aktiivsust üles näitaksid. Nimetatud riske on kirjeldanud Justiitsministeerium esitatud arvamuses.

7.4.2 Karistusõiguslikud probleemid

Justiitsministeerium ja prokuratuur on nõustunud esitatud arvamuses Rahandusministeeriumi varem esitatud seisukohaga, mille kohaselt võivad praegu kehtivad karistusseaduse ruumilise ja isikulise kehtivuse sätted jääda e-residentsuse puhul puudulikeks. Prokuratuur on leidnud,

[34] Vastavalt Euroopa Parlamdendi ja Nõukogu määruse (EL) 2013/575 art 4 lg 1 p 52 on operatsioonirisk - risk saada kahju sisemiste protsesside, inimeste tegevuse ja süsteemide ebaadekvaatse toimimise või mittetoimimise või väliste sündmuste tagajärjel; see hõlmab ka õiguslikku riski. Oma olemuselt on operatsiooniriskid subjektiivse iseloomuga riskid ja seega on operatsiooniriskide problemaatikal otsene seos krediidiasutuse ja kliendi vaheliste ärisuhetega.

[35] Järelevalveasutuste poolt rakendatav järelevalvelise hinnangu protsess (rahvusvaheliselt tuntud akronüümi SREP nime all).

[36] Kuigi e-residendi isikutunnistust ei tohi teisele isikule üle anda, võib see praktikas siiski aset leida (sealhulgas isiku enda teadmata tema identiteeti ära kasutades).

et erinevate majandusalaste kuritegude, muu hulgas rahapesule eelneva kuritegeliku tegevuse puhul on suur ebaõigete andmete ja dokumentide koostamise ja kasutamise oht. Turvaline majanduskeskkond ja võimekus reageerida õigusrikkumistele peab olema tagatud, sh regulatsioonide ja ressursside tasandil. Justiitsministeerium ja prokuratuur nõustuvad Rahapesu Andmebüroo seisukohaga, et olles antud hetkel mahtudelt väike rahapesu transiitriik, siis üheks võimalikuks e-residentsusega kaasnevaks ohuks on suureks rahapesu transiitriigiks saamine.

7.4.3. Haldusõiguslikud probleemid

Justiitsministeeriumi hinnangul on e-residentsusega kaasnev menetlus haldusmenetluse printsiipidest tugevalt kõrvale kalduv ja seetõttu on ka menetlusnormide kooskõla põhiseadusega kaheldav. Haldusaktide ja -toimingute põhjendamiskohustus tuleneb eelkõige hea halduse tavast ja otseselt ka Euroopa Liidu põhiõiguste harta artiklist 41.

7.4.4. Võimalik ebakõla Eesti Vabariigi põhiseadusega

Justiitsministeerium on juba varem isikut tõendavate dokumentise seaduse (edaspidi *ITDS*) eelnõu väljatöötamisel kui ka sellele järgnevates menetlusetappides korduvalt juhtinud tähelepanu probleemile, et ITDS § 20[6] lõigetes 2 ja 3 nimetatud keeldumise alused võivad olla liiga ebamäärased ning koostoimes § 207 nimetatud menetluslike eranditega piirata ülemääraselt Põhiseaduse[37] §-des 14 ja 15 sätestatud isiku õigust menetlusele ja kaebeõigust. Riigi julgeoleku ja avaliku korra kaitsmise eesmärgil võivad sellised piirangud vähemalt e-residendi digitaalse isikutunnistuse instituudi juurutamise etapis ajutiselt olla vajalikud ja mõõdukad, kuid eeldavad siiski HKMS[38] § 79 analüüsi ja täiendamist vastavalt vajadusele.

7.5. Terrorismi leviku suurenemise risk

Majanduse ja julgeoleku olukord maailmas on viimastel aastatel oluliselt muutunud, sealhulgas tänu väga kiirele tehnoloogia arengule. Ekstremismi levik on viimastel aastatel oluliselt kiirenenud. **Rahapesu ja terrorismi rahastamise suurenemine võib omada mõju Eesti Vabariigi julgeolekule, sh riigi rahvusvahelistele suhetele (nt eelkõige USA ja teiste G7 riikidega, kelle jaoks on terrorismi leviku piiramine hetkel üks prioriteetseimaid teemasid)**. Täpsemalt on vastavaid riske ja rahvusvahelisi nõudeid kirjeldatud lisas 3 „Rahvusvaheliste nõuete järgimine, mõju Eesti Vabariigi mainele ning rahvusvahelised arengud“.

7.6. Eesti rahvusvahelise standardi languse ja teiste riikidega suhete halvenemise risk

Näost näkku tuvastamise nõude kaotamise fakt iseenesest, üksikud laia kõlapinda leidvad väärkasutuse juhtumid, kuritegevuse kasv jms võivad mõjutada negatiivselt pankade ja riigi

[37] Eesti Vabariigi põhiseadus, RT I, 27.04.2011, 2, https://www.riigiteataja.ee/akt/127042011002
[38] Halduskohtumenetluse seadustik, RT I, 19.03.2015, 24, https://www.riigiteataja.ee/akt/119032015024

mainet, sh rahvusvahelisi hinnanguid (nt MONEYVALi ja OECD hinnanguid edaspidi Eesti Vabariigi rahapesu ja terrorismi rahastamise tõkestamise süsteemile). Täpsemalt on kirjeldatud rahvusvaheliste nõuete täitmise kohustust ja mõju Eesti Vabariigi mainele lisas 3 „Rahvusvaheliste nõuete järgimine, mõju Eesti Vabariigi mainele ning rahvusvahelised arengud“. Vastavale riskile on muu hulgas viidanud Eesti Pangaliit.

7.7. Halduskoormuse tõus ja sellega seotud mõjud

E-residentidele pangakontode avamise hõlbustamisega võib kaasneda halduskoormuse tõus Politsei- ja Piirivalveametile ja Prokuratuurile juhul, kui tekib rohkem kuritarvitusi, keerukamad kriminaaluurimised ja vaidlused kohtutes (uurijate, prokuröride ja kohtunike töökoormus tõuseb).

Hoolsusmeetmete rakendamine e-residentide puhul on problemaatilisem (näiteks dokumentide digiallkirjastaja tuvastamine), kuna tegemist on mitteresidentidega. Täiendavate hoolsusmeetmete massiline kasutamine suurendab krediidiasutuste kulusid, sh olulisi kulusid seoses pankade sisemiste elektrooniliste monitooringusüsteemide arendamise vajadusega. Samas võib hoolsusmeetmete tugevdatud korras rakendamise mahu oluline kasv vähendada kontrolli kvaliteeti või tekitada olukorra, kus pangad otsustavad näiteks mitteresidente enam üldse mitte teenindada. Vastavalt krediidiasutuste seaduse § 89 lõikele 9 on krediidiasutus vaba otsustama, keda teenindamisele võtta või mitte võtta.[39] Vastavatele riskidele ja mõjudele on viidanud Eesti Pangaliit ja Maailmapanga ekspert.

7.8. Kaugkanalite kaudu loodud õigussuhete kehtima jäämisega seonduvad riskid

E-residentsus on väidetavalt hüve, mille saab igal ajahetkel isikult ära võtta. Samas ei muutu tühiseks selle alusel sõlmitud lepingud. Näiteks kui isik on avanud endale konto ning tellinud PIN-kalkulaatori ja pangakaardi, siis e-residentsuse äravõtmisel jäävad need lepingud kehtima ja kaugkanalid aktiivseks, kuna e-residentsuse äravõtmine ei anna automaatset alust lepingute lõpetamiseks ja ainukeseks mõjuks jääb selle konkreetse vahendi kui allkirjastamis- ja juurdepääsukanali sulgemine.

7.9. eIDAS[40] rakendusaktide puudumisega seonduvad riskid

Siseministeerium on juhtinud tähelepanu eIDAS-e rakendusaktide puudumisega seotud riskikohtadele. Täna on e-identimine (laiemalt isikutuvastamise ja isikusamasuse

[39] Krediidiasutuste seadus, RT I, 19.03.2015, 41, https://www.riigiteataja.ee/akt/119032015041

[40] eIDAS on üks Euroopa digitaalarengu tegevuskava (Digital Agenda) prioriteetidest ja üks Ühtse turu akti (Single Market Act) 12-st põhimeetmest. eIDAS-i eesmärk on suurendada usaldust elektrooniliste tehingute vastu siseturul, luues ühise aluse turvalisele elektroonilisele suhtlusele kodanike, ettevõtjate ja ametiasutuste vahel, nii suurendades avaliku ja erasektori internetipõhiste teenuste ja e-kaubanduse tõhusust Euroopa Liidus. eIDAS jõustus 17.09.2014, kuid sisuliselt ei ole määruse rakendamine veel võimalik. Kuivõrd suur osa määruse jõustumiseks vajalikest rakendusaktidest on väljatöötamisel, rakendub eID kohustuslik tunnustamine 18.09.2018 ning usaldusteenuste osa kohustuslik tunnustamine 1.07.2016.

kontrollimise põhimõtted) ja e-tehingute jaoks vajalikud usaldusteenused Eestis reguleeritud isikut tõendavate dokumentide seaduse ja digitaalallkirja seadusega. Kuivõrd eIDAS rakendusaktid on alles koostamisel, puudub hetkeseisuga täielik ülevaade, kas ja kui suures osas tuleb Eesti siseriiklikke õigusakte muuta.

7.10. Pangakontode registri ja asjakohaste arstimis- ning konfiskeerimismeetmete puudumisega seotud riskid

Tulenevalt rahvusvahelistest nõuetest peab olema tagatud Eesti jätkuv võimekus osutada vastastikust õigusabi ja koostööd rahapesu ja terrorismi rahastamise kaasuste lahendamisel. Muu hulgas peab Eesti olema suuteline kiirelt tuvastama ja jälgima isikute pangakontodega seotud tehinguid (tehingute jälgimise nõue tuleneb Varssavi konventsioonist). E-residentsuse projekti tulemusel võib suureneda pangakontode avamine Eestis, sh mitteresidentide poolt. Seetõttu tuleks kaaluda pangakontode registri loomist.[41] Lisaks oleks vajalik täiendavalt analüüsida kas kehtivad varade arstimis- ja konfiskeerimismeetmed on piisavad e-residentide kontodel liikuvate võimalike „mustade“ rahade arestimiseks ja konfiskeerimiseks. Kaaluda tuleks näiteks pööratud tõendamiskoormuse ehk tsiviilkonfiskeerimise kehtestamise võimalusi.

7.11. Krediidi väljastamisega seotud riskid

RahaPTS § 15 lõikes 1 sätestatud näost näkku tuvastamise nõue on aidanud piirata tarbijate poolt laenude ja liisingute kergekäelist võtmist ja võõra isiku digitaalse isikutunnistuse kuritahtlikku kasutamist.[42] SMS-i ja teiste kaugkanalite kaudu laenude andmine on Eestis väga levinud ja RahaPTS § 15 lõikes 1 sätestatud näost näkku tuvastamise nõue on aidanud kergekälist laenuandmist ja kuritarvitusi piirata.

7.12. Eesti välisesinduste töökoormuse ja põhifunktsioonide muutumisega seotud riskid

Kuna puudub vastav riski ja mõjude analüüs, on raske prognoosida Eesti välisesinduste töökoormuse ja põhifunktsioonide muutmisega seotud riske ja lahendusi. Välisesindustele pankade hoolsusmeetmete rakendamise kohustusi panna ei saa, kuna see tooks kaasa riigile täiendavaid põhjendamatuid kulutusi ja vastutust. Välisesindustel puudub ka vastav oskus sest hoolsusmeetmete rakendamise ulatus ja sisu sõltub panga tuvastatud riskidest ja pakutavate teenuste sisust. Rahapesu ja terrorismi rahastamise tõkestamise meetmete rakendamise lõppvastutajaks peab alati jääma vastava kliendisuhte loonud isik (nt pank), mitte riik.

[41] Hetkel vastav tehniline lahendus puudub, kuid võimalusi on mitmeid, sealhulgas näiteks e-aresti registrile vastavate arenduste loomine ja vajalike seadusandlike muudatuste tegemine RahaPTS-is (nt tuleks sätestada pankade kohustus liituda vastava registriga). Pangakontode registri loomiseks tuleks kõigepealt läbi viia vastav mõjuanalüüs.

[42] Isikutunnistust ei tohi teisele isikule üle anda, kuid praktikas leiavad siiski vastavat juhtumid aset.

Välisministeerium ei ole pankade „letipikenduseks“ hakkamist toetanud.[43] Nimetatud lahendust ei ole toetanud ka teised asutused ja vastava ala eksperdid.

8 E-residentidele pangakonto avamise hõlbustamise võimalused: järeldused ja ettepanekud

Lähtudes käesolevas analüüsis ja selle lisades toodust, saab teha järgmised järeldused ja ettepanekud.

8.1. Üldised järeldused

1. **Eesti rahapesu ja terrorismi rahastamise vastu võitlemise süsteem tugineb eelkõige asjakohastele ennetavatele meetmetele**. **RahaPTS § 15 lõikes 1 sätestatud näost näkku tuvastamise nõue on üheks peamiseks ennetavaks meetmeks, millele tugineb tunne-oma klienti-printsiibi kohaldamine pankade poolt**. Lisaks Eestile on ka teisi riike, kes rakendavad näost näkku tuvastamise printsiipi pangakontode avamisel.[44] **Näost näkku tuvastamise nõude kaotamine või muutmine võib kaasa tuua erinevaid riske, mida on täpsemalt kirjeldatud 7. peatükis**.

2. **Tugevad rahapesu ja terrorismi rahastamise tõkestamise meetmed aitavad hoida Eesti Vabariigi rahandussüsteemi ja majandusruumi usaldusväärsena ning tagada Eesti Vabariigi julgeolek ja iseseisvus**. „Mustad“ rahavood võivad näiteks oluliselt mõjutada ettevõtete ja riigi finantsseisu, mis omakorda võivad mõjutada sõltumatust teistest.

3. **Kliendi näost näkku tuvastamise nõue konto avamisel toetab krediidiasutuste avalik-õiguslike kohustuste täitmist**. Käesolevast analüüsist nähtub, et krediidiasutustel on palju erinevaid avalik-õiguslikke kohustusi, mida on võimalik efektiivselt täita vaid juhul, kui krediidiasutusel on olemas kliendi isikuandmed ja seadusandjad on andnud krediidiasutustele õigusliku võimaluse saada võimalikult täpset teavet kliendi isiku identiteedi ja residentsuse, tema majandusliku seotuse ning tehingute eesmärkide kohta. **RahaPTS-i 15 lõikes 1 toodud näost näkku tuvastamise nõue on siiani aidanud kaitsta mitmel moel Eesti majandus ja rahandussüsteemi, sh riskide eest, mis on rahapesu ja terrorismi rahastamisega kaudsemalt seotud (nt pankade kapitali- ja likviidsusriskid)**.

4. **Mitteresidentidele orienteeritud pangandus- ja majanduspoliitika, samuti *off-shore*-äri soodustamine, kätkeb endas mitmeid olulisi ohte ja haavatavusi pankadele ja riigile tervikuna**. Näost näkku isiku tuvastamise nõude kaotamine võib soodustada

[43] Vastavat ideed on arutatud lisaks Rahandusministeeriumis toimunud ümarlaua ja e-residentsuse projekti nõukoja koosoleku raames.
[44] nt Tšehhi, Sloveenia, Horvaatia ja Ungari. Täpsemalt vt lisa 5 „Näited teiste riikide seadusandlustest ja praktikast“.

mitteresidentidele orienteeritud pangandust. Lisaks võimaldatakse E-residentsuse projekti raames mitteresidentidel lihtsalt registreerida Eestis äriühinguid, millel ei pruugi alati olla majanduslikku seoseost Eesti Vabariigiga. Teiste riikide praktikast nähtub, et taoline mitteresidentidele orienteeritud pangandus- ja majanduspoliitika, sealhulgas *off-shore* äri soodustamine, kätkeb endas mitmeid olulisi ohte ja haavatavusi pankadele ja riigile. **Kolmandate riikide klientide arvu suurenemine finantsasutustes (eelkõige pankades) võib omada nii likviidsus- kui ka operatsioonioriskile suurendavat mõju. Mitteresidentide hoiused on volatiivsemad kui residentide oma. Võimaliku maksejõuetuse korral kannab hoiuste tagamise riski Eesti hoiuste tagamise fond, sõltumata kliendi residentsusest. Operatsioonioriski[45] realiseerumine rahapesu valdkonnas võib pangasektoris kaasa tuua tagajärjed finantssektori usaldusväärsusele (sh tõrked teiste pankadega rahvusvahelistes korrespondentsuhetes ja reputatsioonirisk); konkreetse krediidiasutuse puhul võib operatsioonioriski realiseerumine väljenduda ka kõrgemas kapitalinõudes (läbi SREP[46] hinnangute).**

5. **Kuivõrd eIDAS[47] rakendusaktid on Euroopa Liidus alles koostamisel, puudub hetkeseisuga täielik ülevaade, kas ja kui suures osas tuleb Eesti siseriiklikke õigusakte muuta.**

6. **E-residentidega ärisuhte loomisel, sh pangakonto avamisel, tuleb rakendada hoolsusmeetmeid tugevdatud korras, kuna kontakt luuakse üldjuhul distantsilt ja tegemist on mitteresidentidega**.[48] Mitteresidendid kõrgema rahapesu ja terrorismi rahastamise riskiga kliendid, kellele konto avamisel tuleb kohaldada hoolsusmeetmeid tugevdatud korras, et ennetada võimalikke kuritarvitusi.

8.2. E-residentidele pangakonto avamise hõlbustamise võimalused

8.2.1. E-residentidele pakutavad teenused ja nendega seotud riskid

E-residentsust on võimalik taotleda kõigil välismaalastel, kes soovivad Eesti e-teenuseid kasutada. **Aastaks 2025 on maailmas oodatavalt kokku 10 miljonit e-eestlast ehk e-**

[45] Vastavalt Euroopa Parlamdendi ja Nõukogu määruse (EL) 2013/575 art 4 lg 1 p 52 on operatsioonirisk - risk saada kahju sisemiste protsesside, inimeste tegevuse ja süsteemide ebaadekvaatse toimimise või mittetoimimise või väliste sündmuste tagajärjel; see hõlmab ka õiguslikku riski. Oma olemuselt on operatsioonioriskid subjektiivse iseloomuga riskid ja seega on operatsioonioriskide problemaatikal otsene seos krediidiasutuse ja kliendi vaheliste ärisuhetega.

[46] Järelevalveasutuste poolt rakendatav järelevalvelise hinnangu protsess (rahvusvaheliselt tuntud akronüümi SREP nime all).

[47] eIDAS on üks Euroopa digitaalarengu tegevuskava (Digital Agenda) prioriteetidest ja üks Ühtse turu akti (Single Market Act) 12-st põhimeetmest. eIDAS-i eesmärk on suurendada usaldust elektrooniliste tehingute vastu siseturul, luues ühise aluse turvalisele elektroonilisele suhtlusele kodanike, ettevõtjate ja ametiasutuste vahel, nii suurendades avaliku ja erasektori internetipõhiste teenuste ja e-kaubanduse tõhusust Euroopa Liidus. eIDAS jõustus 17.09.2014, kuid sisuliselt ei ole määruse rakendamine veel võimalik. Kuivõrd suur osa määruse jõustumiseks vajalikest rakendusaktidest on väljatöötamisel, rakendub eID kohustuslik tunnustamine 18.09.2018 ning usaldusteenuste osa kohustuslik tunnustamine 1.07.2016.

[48] Täpsemalt lisas 1 „Kontosuhte regulatsioon“, lk 8-11.

residenti. E-residentsus annab välisriikides elavatele välismaalastele Eesti elanikega sarnased võimalused Eesti e-keskkonnas tegutsemiseks, sh allkirjastada dokumente ja kasutada erinevaid teenuseid, sh äriühingu registreerimine ja pangakontode avamine Eestis. Nii on e-residendil võimalik registreerida äriühing Eestis ning osaleda aktiivselt selle juhtimises, elades ise mujal.[49]

Rahapesu ja terrorismi rahastamisega seotud riskid on äriühingu registreerimisel ning pangakontode avamise ja kasutamise teenusel. Pangakontode avamise ja kasutamiseg seotud riske on analüüsitud täpsemalt 7. peatükis.

8.2.2. E-residentidele pangakontode avamise hõlbustamise eeldused

E-residentidele pangakonto avamise hõlbustamise võimaldamise eelduseks on käesolevas analüüsis nimetatud juriidiliste ja tehniliste kitsaskohtade lahendamine. Soovitav on enne RahaPTS-is asjakohaste muudatuste tegemist täiendada e-residentsuse taotlemise menetlemise protsessi täiendavate meetmetega, et ennetada võimalikke kuritarvitusi ning asjakohaste asutuste halduskoormuse suurenemist. **Kaaluda** tuleks järgmiste täiendavate meetmete kohaldamist.[50]

1) Teostada taustakontroll rahvusvaheliste sanktsioonide nimekirjade suhtes.[51]
2) Kehtestada e-residentsuse taotlejatele nõue esitada Politsei- ja Piirivalveameti nõudmisel[52] enda elukohariigi või -riikide karistusregistri tõend või pädeva kohtu- või haldusorgani väljastatud samaväärse dokument, mis tõendab karistuse puudumist ja mille väljastamisest ei ole möödunud rohkem kui kolm kuud ning mis on vajadusel notariaalselt või sellega võrdsustatud korras kinnitatud ja legaliseeritud või kinnitatud legaliseerimist asendava tunnistusega (*apostille*'iga), kui välislepingust ei tulene teisiti.[53]
3) Kehtestada e-residendi kaardi taotlejale kohustus esitada telefoninumber, e-mail, Skype ja Facebooki konto (olemasolul) ning tagada pankadele ärisuhte loomisel õigus saada vastavaid andmeid elektroonilise päringu (X-tee) alusel.[54]
4) Kehtestada põhjalikum kontrollmehhanism e-residentsuse taotlemise põhjuste kontrollimiseks ja esitatud andmete järelkontrollimiseks (nt kontrollida väidetud seotus Eestiga).[55]

[49] Täpsem info Majandus ja Kommunikatsiooni ministeeriumi kodulehel: https://www.mkm.ee/et/eesti-alustas-e-residentsuse-programmiga.
[50] Loetelus on arvestatud Eesti Pangaliidu ettepanekuid.
[51] Eestis tuleb rakendada sanktsioone, mille on kehtestanud ÜRO ja Euroopa Liit ning need sanktsioonid ei piirdu ainult reisikeeluga.
[52] Politsei- ja Piirivalveametil võib kogutud andmete põhjal tekkida vajadus kontrollida e-residentsust taotleva isiku kriminaalse tausta puudumist.
[53] Tuleks ära defineerida riskiriigid või profiilid, kelle puhul sellist nõuet rakendatakse. Lisadokumentide küsimine tekitab Politsei- ja Piirivalveametile lisakoormust ning seega tuleks sellisel juhul arvestada menetlustähtaja pikendamisega.
[54] Haldusmenetluse raames kogutud andmeid ei saa üldjuhul erasektoriga jagada, mistõttu tuleks kaaluda e-residentidelt vastavate andmete kogumist muus vormis – näiteks võetakse e-residentidelt isikuandmete edastamise nõusolek Digi-ID taotlemisel). Antud võimalusi tuleks täiendavalt analüüsida koostöös Andmekaitse Inspektsiooniga.

5) väljastada digi-ID ainult välisriigis väljaantud kehtiva isikut tõendava või reisidokumendi alusel mis kehtib vähemalt 6 kuud arvates selle esitamisest.

8.2.3. E-residentidele pangakontode avamise hõlbustamise võimalused

Käesolevast analüüsist nähtub, et RahaPTS § 15 lõikes 1 sätestatud näost näkku tuvastamise nõue omab väga mitmeid positiivseid mõjusid. Teiste riikide seaduste ja praktika analüüsist nähtub, et nimetatud nõue on seaduse tasandil kehtiv ka mitmes teises riigis. Lisaks näitas analüüs, et mitteresidentide puhul tuleb kohaldada hoolsusmeetmeid tugevdatud korras olenemata asjaolust, kas konto avatakse vahetu kontaktita või kohtudes näost näkku. Nimetatud hoolsusmeetmeteks on enamikul juhtudel näiteks nõue, et esimene makse kliendi kontole tehakse sama kliendi nimel olevalt kontolt sarnaseid hoolsusmeetmeid rakendavas pangas. Samuti jägitakse mitteresidentide puhul keskmisest rangemalt nende kontoga seotud tehinguid ning küsitakse vajadusel täiendavaid tõendeid konto omaniku tausta ja tema kontol olevate rahaliste vahendite päritolu kohta.[56]

Lähtudes eeltoodust, ei ole Rahandusministeeriumi hinnangul mõistlik seoses e-residentidele pangakontode avamise hõlbustamise vajadusega muuta RahaPTS § 15 lõikes 1 sätestatud näost näkku tuvastamise printsiipi, mis on olnud üheks peamiseks ja tugevaimaks ennetavaks meetmeks Eesti Vabariigi rahapesu ja terrorismi rahastamise tõkestamise süsteemis. Selle asemel oleks tuvastatud riske paremini maandavaks lahenduseks kehtestada e-residentidele erand, mis sätestab järgmised asjakohased täiendvad hoolsusmeetmed võimalike väärkasutuste ennetamiseks.

E-residentidele, keda pole näost näkku tuvastatud, tuleks konto avada üksnes juhul, kui:[57]

1) isikul on mõjuv põhjus Eestis konto avamiseks, sh selgitatakse välja tehingute eesmärk;[58]
2) isikusamasuse kontrollimiseks kasutatakse infotehnoloogilisi vahendeid, mille pildi- ja helikvaliteet võimaldab kontot avada sooviva isikuga suhelda vahetult, võrrelda tema nägu esitatud isikut tõendava dokumendil oleva pildiga, kontrollida e-residentsuse kaardi olemasolu ja viia läbi muud toimingud isiku tausta, rahaliste vahendite ja varade päritolu ning tehingu eesmärgi kontrollimiseks (nn tunne-oma-klienti-printsiibi täitmine);
3) punktis 2) toimingud tuleb salvestada;[59]
4) avatavale kontole tehakse esimene makse samale isikule kuuluva konto kaudu, mis on avatud krediidiasutuses, kellel on tegevuskoht Euroopa Majanduspiirkonna lepinguriigis või riigis, kus kehtivad RahaPTS-iga võrdväärsed nõuded;

---

[55] Politsei- ja Piirivalveamet vajaks tõenäoliselt selliseks lisategevuseks lisaressursse.
[56] Nimetatud nõuded tulenevad asjakohastest rahvusvahelistest standarditest.
[57] Lisaks nimetatud lisameetmetele tuleb rakendada ka RahaPTS-is toodud muid hoolsusmeetmeid, sh nt andmete säilitamise kohustus jne.
[58] Vastavaid täiendavaid selgitusi küsib ja kontrollib konto avamisel pank.
[59] Perioodi täpne pikkus on kaalumisel, kuid tõenäoliselt on perioodiks mitte vähem kui 6 kuud.

5) kontole kantavate rahaliste vahendite päritolu kontrollitakse ja jälgitakse tugevdatud korras ning nimetatud nõuded täpsustatakse võimalusel rahandusministri määruses;[60]
6) e-residendist füüsilise isiku ja e-residendi poolt registreeritud juriidilise isiku isikusamasuse tuvastab, vastavad andmed kogub ja säilitab krediidiasutus RahaPTS-i 2. jaos toodud korras. Täiendavalt kogutakse ja säilitatakse e-residendi isikut tõendava dokumendi koopia, mille isikuandmete ja fotoga leheküljest tehakse koopia.[61]

8.2.4. Täiendavad ettepanekud

Täiendavalt tuleks kaaluda järgmiste meetmete kehtestamist ja/või vajalikke tegevusi:

1) e-residendile väljastatud Digi-ID kehtivuse kontrollimise võimaldamine (nt pankadele ärisuhte loomisel, notaritele jne) vastava registri kaudu (nt Rahvastikuregister) või muul võimalikul kujul;[62]
2) auditeerimiskohustuse kehtestamine e-residendi poolt registreeritud äriühingule, kelle on avatud konto Eestis;[63]
3) e-residentsuse programmi eestvedajatel kaardistada vajalikud tegevused, sh riskide ja kitsaskohtade lahendamiseks, ja esitada asjakohaste tegevuste läbiviimiseks vajalike rahaliste kulutuste täpne prognoos riigi eelarvest vajalike vahendite hankimiseks.

[60] Koostöös Pangaliidu ja asjakohaste asutustega tuleks kaaluda näiteks summaliste ja sularaha väljavõtmisega seotud piirangute kehtestamist, kuna Eestil on väga kõrged rahapesu riskid seoses näiteks idasuunaliste sularaha voogudega.

[61] E-residendi kaart ei ole isikut tõendav ega reisidokument ning sellel puudub isiku pilt. Politsei- ja Piirivalveameti poolt esitatud andmetel ei säilitada e-residendi digi-ID menetluse raames alati koopiat esitatud isikut tõendavast dokumendist elektroonsel kujul Politsei- ja Piirivalveameti infosüsteemis. Seega ei ole võimalik elektroonsel teel esitatud dokumendi koopiat päringuga tagastada. Politsei- ja Piirivalveamet kannab oma infosüsteemi andmed dokumendi kohta (liik, nr, kehtivusaeg, väljaandja) ning neid saaks tehniliselt vajadusel hakata X-tee päringuga väljastama ka pankadele. Kaaluda võiks infosüsteemide arendamist selliselt, et kõik digi-ID menetluse raames kogutud dokumendid oleks skänneeritud Politsei- ja Piirivalveameti infosüsteemi, et neid X-tee päringuga väljastada ka pankadele.

[62] Notaritel ja pankadel on juurdepääs rahvastikuregistrile olemas. Siseministeeriumi rahvastikutoimingute osakonnal on kohe kooskõlastamisele minev eelnõu, millega hakatakse e-residentide kohta andmeid koguma ja sellisel juhul on neil juurdepääs andmetele olemas.

[63] Auditeerimiskohustus aitaks tõenäoiselt ennetada e-residentide poolt nn riiulifirmade loomist.