Virtuaalivaluutan tarjoajien rahanpesun ja terrorismin rahoittamisen riskiarvion yhteenveto

26.11.2024

Sisällys

Lyhyesti

Finanssivalvonta on laatinut sektorikohtaisen riskiarvion sen valvottaviin virtuaalivaluutan tarjoajiin liittyvistä rahanpesun ja terrorismin rahoittamisen riskeistä.

Riskiarvion mukaan sektoriin kokonaisuudessa kohdistuva sekä rahanpesun että terrorismin rahoittamisen riski on merkittävä eli toiseksi korkein neljäportaisella tasolla.

Reaaliaikaisuus ja globaali liikkuvuus kohottavat virtuaalivaluuttoihin liittyvää riskiä sekä rahanpesun että terrorismin rahoittamisen näkökulmasta. Näin ollen myös virtuaalivaluuttoihin liittyvien palvelujen tarjoamiseen liittyy riski siitä, että palveluiden kautta siirretään rikoksella hankittuja varoja globaalisti ja nopeasti.

Finanssivalvonnan säännöllisesti keräämien tietojen sekä valvontatoimenpiteiden myötä on lisäksi havaittu, että virtuaalivaluutan tarjoajien riskienhallintakeinoissa on puutteita.

1 Sektorikohtaisen riskiarvion tarkoitus ja soveltamisala

Virtuaalivaluutan tarjoajia koskeva sektorikohtainen rahanpesun ja terrorismin rahoittamisen riskiarvio on Finanssivalvonnan arvio virtuaalivaluutan tarjoajiin sektoritasolla kohdistuvista rahanpesun ja terrorismin rahoittamisen riskeistä. Finanssivalvonnan rahanpesun ja terrorismin rahoittamisen ominaisriskiarviossa eri sektoreihin liittyviä riskejä on tarkasteltu ylätasolla ja ainoastaan sektoreille tyypillisesti tarjottavien tuotteiden ja palveluiden näkökulmasta. Sektorikohtaista riskiarviota varten on perehdytty syvällisemmin virtuaalivaluutan tarjoajista säädetyn lain (572/2019) mukaan rekisteröityneiden virtuaalivaluutan tarjoajien tuotteisiin ja palveluihin, asiakkaisiin, jakelukanaviin sekä maantieteelliseen kattavuuteen. Lisäksi on otettu huomioon myös riskienhallintakeinot. Arvio muodostetaan kuitenkin sektoritasolla, ei yksittäisten valvottavien tasolla.

Riskiarvio ohjaa Finanssivalvontaa suuntamaan valvontaresursseja ja valitsemaan valvontatoimenpiteet riskiperusteisesti. Euroopan pankkiviranomaisen (jäljempänä EBA) riskiperusteista valvontaa koskevan ohjeen mukaisesti Finanssivalvonnan tulee laatia rahanpesun ja terrorismin rahoittamisen estämisen valvontastrategia, jonka keskeisenä osana ovat eri valvottavasektoreita koskevat riskiarviot.

Virtuaalivaluutan tarjoajia koskeva sääntely on muuttunut merkittävästi vuoden 2024 aikana. Asetus (EU) 2023/1114 kryptovarojen markkinoista (eng. *markets in crypto-assets*, jäljempänä *MiCA-asetus*) annettiin 31.5.2024. MiCA -asetuksen takia säädettiin uusi laki kryptovarapalvelun tarjoajista ja kryptomarkkinoista (402/2024), joka tuli voimaan 30.6.2024 ja kumosi lain virtuaalivaluutan tarjoajista. Virtuaalivaluutan tarjoajia koskevaan rekisteriin merkittyjen toimijoiden tulee hakea MiCA-asetuksen mukaista toimilupaa, mikäli ne aikovat jatkaa palveluiden tarjoamista.

Tämä riskiarvio kuvaa sektorin tilannetta sääntelyn murroskohdassa eli elokuussa 2024, jolloin Finanssivalvonnan rekisteriin oli merkitty 13 virtuaalivaluutan tarjoajaa eikä yhtään uuden sääntelyn mukaista toimilupahakemusta ollut vielä vastaanotettu. Rekisteriin merkityistä kuusi on rekisteröity jo kansallisen lain voimaan tultua vuonna 2019 ja loput sen jälkeen.

Kuten jo säädösten nimistä käy ilmi, eurooppalaisen sääntelyn myötä tullaan jatkossa virtuaalivaluutan sijaan käyttämään termiä *kryptovarat* ja virtuaalivaluutan tarjoajan (eng. *Virtual Asset Service Providers,* jäljempänä *VASP*) sijaan käytetään termiä kryptovarapalvelun tarjoaja (eng. *Crypto Asset Service Provider*, jäljempänä *CASP*).

Koska kyse on vielä vanhan sääntelyn nojalla myönnetyistä rekisteröinneistä, käytetään tässä riskiarviossa vanhan sääntelyn mukaisia termejä eli virtuaalivaluutan tarjoaja (VASP) ja virtuaalivaluutta.

2 Riskiarvion laatiminen

Finanssivalvonta käyttää rahanpesun ja terrorismin rahoittamisen riskejä arvioidessaan neliportaista asteikkoa, joka vastaa Euroopan pankkiviranomaisen käyttämää arviointiasteikkoa[1]. Jokaista riskitasoa kuvaamaan on määritelty sitä vastaava riskipiste.

Riskitaso	Riskitasoa vastaava riskipiste
Erittäin merkittävä	4
Merkittävä	3
Melko merkittävä	2
Vähemmän merkittävä	1

Sektorikohtainen riskiarvio laaditaan arvioimalla seuraaviin riski- ja hallintakeinokategorioihin liittyvä riskitaso:

- Riskikategoriat:
  - Tuotteet ja palvelut
  - Maantieteellinen sijoittautuminen
  - Asiakkaat
  - Jakelukanavat
- Hallintakeinokategoriat:
  - Toiminnan riskiperusteisuus
  - Toiminnan organisointi
  - Asiakkaan tunteminen
  - Monitorointi

Sekä riski- että hallintakeinokategoriat arvioidaan sen mukaan, kuinka suuri riski niihin liittyy. Myös hallintakeinojen osalta huomio kohdistuu hallintakeinojen puutteisiin ja näiden puutteiden riskiä nostavaan vaikutukseen.

Kokonaisriskitaso on riskikategorioiden ja hallintakeinokategorioiden riskitasoista muodostettu yhteisarvio. Riskikategorioiden riskitasoa on painotettu enemmän suhteessa hallintakeinokategorioihin. Syynä tähän on se, että rahanpesun tai terrorismin rahoittamisen riskiä ei voi eikä aina ole tarkoituksenmukaistakaan pyrkiä poistamaan kokonaan hallintakeinoilla. Lisäksi käsitys hallintakeinoista perustuu suurilta osin valvottavien RA-tiedonkeruulla[2] raportoimiin tietoihin, joita ei ole todennettu valvontatoimenpitein.

Riskiarviota laadittaessa on hyödynnetty muun muassa seuraavia tietoja

- VASP:ien rekisteröinnin yhteydessä Finanssivalvonnalle toimittamat tiedot, RA-tiedonkeruulla raportoimat tiedot (tiedon ajankohdalla 31.12.2023) sekä valvontatoimenpiteiden yhteydessä saadut tiedot.
- Keskusrikospoliisin rahanpesun selvittelykeskuksen vuosikertomukset sekä viranomaisyhteistyössä saadut tiedot.
- FATF:n Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2021) sekä Virtual Asset Contact Group:n kokoukset
- European Banking Authority

[1] EBA The Risk-Based Supervision Guidelines EBA/GL/2021/16, luku 4.3.6

[2] Finanssivalvonnan vuosittainen Rahanpesun ja terrorismin rahoittamisen sekä pakotteita koskevien riskien ja kontrollien tiedonkeruun (RA, Riskiarviokysely)

  - Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector. Paris, France 2023
  - Rahanpesun ja terrorismin rahoituksen riskitekijöitä koskevat ohjeet EBA/GL/2021/02 mukaan lukien muutokset EBA/GL/2024/01
- REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM (2022) 554 final) ja (COM (2019) 370 final)
- Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2021 (Valtiovarainministeriön julkaisuja 2021:12) sekä riskiarvio 2023 Osittaispäivitys (Valtiovarainministeriön julkaisuja 2024:8)

3 Riskiarvio ja sen perustelut

3.1 Sektorikohtaisen riskiarvion tulokset

Finanssivalvonta on arvioinut, että rahanpesun ja terrorismin rahoittamisen kokonaisriski on virtuaalivaluutan tarjoajien sektorilla **merkittävä**.

Kokonaisriski on sama sekä rahanpesun että terrorismin rahoittamisen näkökulmasta. Tämä perustuu siihen, että käytännössä samat elementit tuotteissa ja palveluissa nostavat sekä rahanpesun että terrorismin rahoittamisen riskiä. Maantieteellisen riskin, asiakkaiden ja jakelukanaviin liittyvien riskien osalta sektorikohtaisen riskiarvion tasolla ei ole toistaiseksi eroteltu rahanpesua ja terrorismin rahoittamista toisistaan. Syynä tähän on se, ettei sektoritasolla ole mahdollista käydä läpi esimerkiksi maksuliikennettä maakohtaisesti sen määrittämiseksi, kohdistuuko maksuliikennettä alueille, joihin liittyy kohonnut terrorismin rahoittamisen riski. Yksityiskohtaisempi analyysi voidaan tehdä osana valvottavakohtaisia riskiarvioita, jotka puolestaan voidaan myöhemmin ottaa huomioon sektorikohtaista riskiarviota päivitettäessä. Myös hallintakeinojen osalta rahanpesun ja terrorismin rahoittamisen hallintakeinoja on arvioitu yhtenä kokonaisuutena.

Riskiarviossa on painotettu tuotteisiin ja palveluihin liittyvää riskiä suhteessa muihin riskitekijöihin. Perusteluna tälle on se, että tuotteet ja palvelut määrittävät sen, miten sektoria, alasektoria tai yksittäistä toimijaa voidaan käyttää hyväksi rahanpesuun tai terrorismin rahoittamiseen. Ilman tuotteita tai palveluita, joihin liittyy rahanpesun tai terrorismin rahoittamisen riski, sektorin on vaikea tulla hyväksikäytetyksi rahanpesuun tai terrorismin rahoittamiseen.

Riski- ja hallintakeinokategorioille määritettyjä riskitasoja vastaavat riskipisteet on esitetty alla olevassa taulukossa:

Riskikategoriat:	
Tuotteet ja palvelut	4
Maantieteellinen sijoittautuminen	2
Asiakkaat	3
Jakelukanavat	3
Riskikategorioiden riskitaso:	**3**
Hallintakeinokategoriat	
Riskiperusteisuus	3
Toiminnan organisointi	3
Asiakkaan tunteminen	4
Monitorointi	3
Hallintakeinokategorioiden riskitaso:	**3**
Sektorin kokonaisriskitaso	**3**

3.2 Riskikategoriat

3.2.1 Tuotteet ja palvelut

Tarjottavilla tuotteilla ja palveluilla on ratkaiseva merkitys siinä, mikä on sektorin tai yksittäisen toimijan riski tulla hyväksikäytetyksi rahanpesussa.

Tuotteisiin ja palveluihin liittyvien riskien arvioinnin lähtökohtana on Finanssivalvonnan rahanpesun ja terrorismin rahoittamista koskeva ominaisriskiarvio ja siinä eri tuotteille ja palveluille määritetyt ominaisriskitasot. Finanssivalvonnan vuonna 2022 julkaisemassa ominaisriskiarviossa virtuaalivaluuttapalveluihin liittyvä sekä rahanpesun että terrorismin rahoittamisen ominaisriskitaso on arvioitu merkittäväksi.

Virtuaalivaluuttoja on mahdollista siirtää lähes tai kokonaan reaaliaikaisesti ja minne tahansa maailmassa. Reaaliaikaisuuden vaikutuksia tehostavat erityisesti laajalti käytössä olevat automaattiset kaupankäyntibotit. Lisäksi hyväksytyt transaktiot ovat peruuttamattomia. Kyse on lähes yksinomaan verkossa tapahtuvista transaktioista, jotka toteutetaan ilman osapuolten kasvokkaista kohtaamista. Virtuaalivaluuttoja voi siirtää ja tallettaa hyödyntäen virtuaalivaluuttoihin liittyvien palveluiden tarjoajia, mutta toisaalta yksityishenkilöt voivat siirtää varoja toisilleen myös ilman palveluntarjoajan myötävaikutusta. Näin ollen virtuaalivaluutta toimii ikään kuin sähköisenä käteisenä, jota voidaan liikuttaa globaalisti ilman rajoituksia. Palveluntarjoajaa tarvitaan kuitenkin käytännössä aina virtuaalivaluutan vaihtamiseksi fiat-valuuttaan ja toisinpäin. Globaaleilla markkinoilla on useita tällaiseen toimintaan erikoistuneita palveluntarjoajia, jotka eivät noudata esimerkiksi asiakkaan tuntemista koskevia sääntöjä. Myös rahanpesun selvittelykeskus on omassa analyysissään todennut, että virtuaalivaluuttatoimialan erityispiirteitä ovat nopeat siirrot ja toiminnan kansainvälisyys. [3]

Reaaliaikaisuus ja globaali liikkuvuus kohottavat virtuaalivaluuttoihin liittyvää riskiä sekä rahanpesun että terrorismin rahoittamisen näkökulmasta. Oman haasteensa tuo myös se, että sektoria koskevaa sääntelyä on ollut olemassa vasta lyhyen aikaa ja eteenkin muu kuin rahanpesun ja terrorismin rahoittamisen estämisen osalta se on ollut varin kevyttä. Alalla tarjotaan palveluita globaalisti rajat ylittäen eikä valvontavastuun määrittäminen ja valvonnan järjestäminen ole aina helppoa.

Rahanpesun ja terrorismin rahoittamisen tekotavat virtuaalivaluuttapalvelujen osalta vastaavat pitkälti pankki- ja maksupalvelusektorilla tunnistettuja tekotapoja: varojen rikollinen alkuperä pyritään häivyttämään siirtämällä virtuaalivaluuttaa lompakosta ja palvelusta toiseen sekä tallettamalla ja nostamalla varoja fiat-valuutaksi. Kuten edellä on todettu, oman haasteensa tuo se, että varoja voi siirtää myös valvottujen palveluntarjoajien ulkopuolelta.

Terrorismin rahoittamisen ilmiönä on tunnistettu varojen kerääminen terroristiorganisaatioille virtuaalivaluuttoina. Varoja on kerätty yksinkertaisesti ilmoittamalla sosiaalisessa mediassa lompakko-osoitteita, joihin varoja voi lähettää.

Virtuaalivaluuttaan liittyviä palveluita ovat virtuaalivaluutan tarjoajista säädetyn lain 2 §:n 1 momentin 6 kohdan mukaan virtuaalivaluutan liikkeeseenlasku, virtuaalivaluutan vaihtopalvelu ja lompakkopalvelu. Rekisteröityneet VASP:t tarjoavat joko vaihtopalvelua tai/ja lompakkopalvelua. Palvelukohtaisesti sekä rahanpesun että terrorismin rahoittamisen riski on vaihtopalvelun osalta merkittävä. Rahanpesun riski on myös lompakkopalvelun osalta merkittävä. Terrorismin rahoittamisen riski voidaan katsoa olevan hieman alhaisempi sellaisten lompakkopalveluiden kohdalla, joihin varoja voi siirtää ainoastaan lompakon omistaja eli palveluntarjoajan tunnistettu ja todennettu asiakas.

[3] Rahanpesun selvittelykeskuksen vuosikertomus 2022, s. 17.

Sektorilla toimivien VASP:ien tuotteet ja palvelut sekä näihin tuotteisiin ja palveluihin liittyvät EBA:n riskitekijöitä koskevissa ohjeissa (EBA/GL/2024/01) tarkoitetut riskiä lisäävät tekijät huomioiden tuotteiden ja palveluiden riski kokonaisuudessaan on **erittäin merkittävä.**

3.2.2 Maantieteelliseen sijoittautumiseen liittyvä riski

Maantieteelliseen sijoittautumiseen liittyvä riski on arvioitu olevan **melko merkittävä**.

Kansallinen sääntely ei ole antanut mahdollisuutta kotimaisille VASP:eille tarjota rekisteröintinsä nojalla palveluita muihin EU- tai EU:n ulkopuolisiin maihin. Tarjotakseen virtuaalivaluuttapalveluita muualla kuin Suomessa, Suomeen rekisteröityneiden VASP:ien on tullut hakea toimilupaa tai rekisteröityä kohdemaan sääntelyn edellyttämällä tavalla. Osalla rekisteriin merkityistä VASP:sta on konsernirakenteen johdosta yhteyksiä EU-alueelle, jolloin maantieteellinen riski kohoaa verrattuna puhtaasti kansalliseen toimintaa. Osalla VASP:sta on myös muun toimiluvan nojalla lupa tarjota osaa palveluistaan rajan yli ETA-alueella.

3.2.3 Asiakasriski

Asiakkaisiin liittyvä riski on arvioitu olevan **merkittävä**.

Asiakkaisiin liittyvää riskiä arvioitaessa on otettu huomioon RA-tiedonkeruulla raportoidut tiedot eri asiakasryhmistä. Huomioon on otettu sekä absoluuttisia että prosentuaalisia asiakasmääriä esimerkiksi korkean riskin asiakkaiden ja ulkomaille sijoittautuneiden asiakkaiden osalta. Riskiin on vaikuttanut myös se, mikäli valvottavat eivät ole tunnistaneet korkean riskin asiakkaita.

3.2.4 Jakelukanavariski

Jakelukanaviin liittyvä riski on arvioitu olevan **merkittävä**.

Riskiin on vaikuttanut muun muassa se, että sektorilla palveluita tarjotaan etäasioinnin kautta ilman asiakkaan henkilöllisyyden todentamista rahanpesulain 11 §:n 1 momentin 3 kohdassa tarkoitettua todentamista käyttäen. VASP:t hyödyntävät palveluita tarjotessaan ulkomaisia yhteistyökumppaneita, joiden riskienhallintakeinoista VASP:lla ei välttämättä ole kattavaa käsitystä.

3.3 Hallintakeinokategoriat

3.3.1 Riskiperusteisuus

RA-tiedonkeruulla VASP:t ovat raportoineet ottaneensa huomioon kaikki sääntelyn edellyttämät osa-alueet riskiarviossaan ja luokittelevansa asiakkaat riskiluokkiin. Valvonnassa on käynyt ilmi, että osalla valvottavista riskiarvio jää pinnalliseksi ja asiakkaiden riskiluokittelu perustuu vain yksittäisiin riskitekijöihin. Lisäksi asiakkaalle määritetty riskiluokka ei välttämättä aina vastaa yhtiön riskiarviossa tunnistettuja riskejä. Riskiarviossa tulisi kattavasti käydä läpi valvottavan toimintaan liittyviä rahanpesun ja terrorismin rahoittamisen riskejä ja tunnistetut riskit tulisi ottaa huomioon määritettäessä asiakkaan riskiluokkaa sekä jatkuvan seurannan toimenpiteitä.

3.3.2 Toiminnan organisointi

RA-tiedonkeruulla VASP:t ovat raportoineet laatineensa tai päivittäneensä rahanpesun ja terrorismin rahoittamisen estämistä koskevat toimintaperiaatteet, menettelytavat ja työohjeet viimeisen kahden vuoden aikana. Valvonnassa on kuitenkin havaittu, että ohjeistuksissa ei aina ole riittävän yksityiskohtaisesti ja käytännönläheisesti yksilöity niitä

toimenpiteitä, joita asiakkaiden tuntemisen velvoitteiden noudattaminen edellyttää. Tämä johtaa siihen, ettei asiakkaan tuntemisen velvoitteita välttämättä noudateta yhdenmukaisesti. Myös tehtävien organisointi valvottavissa on osoittautunut puutteelliseksi. Velvoitteiden noudattamisen valvontaan ja seurantaan liittyvät vastuut eivät aina ole selkeästi määritettyjä.

3.3.3 Asiakkaan tunteminen

Asiakkaan tuntemiseen liittyvien hallintakeinojen kohdalla voidaan todeta, että VASP:lla on käytössään erilaisia etätunnistamisratkaisuja asiakassuhteen perustamisessa. Nämä ratkaisut eivät ole rahanpesulain 3 luvun 11 §:n 1 momentin 3 kohdassa tarkoitettuja tunnistustapoja. Niin sanottujen innovatiivisten tunnistamisratkaisujen yhteydessä tulisi noudattaa EBA:n aiheesta antamia ohjeita. Valvonnassa on todettu, että VASP:t eivät aina ole riittävästi perehtyneet siihen, miten niiden käyttämät etätunnistamisratkaisut toimivat. VASP:t ovat myös raportoineet ulkoistaneensa asiakkaan tuntemisen toimia ja käyttävänsä kolmansia osapuolia ilman, että prosesseja ja vastuukysymyksiä on kuvattu yksityiskohtaisesti. Asiakkaiden tuntemistietojen päivittämisessä sekä tehostetun tuntemisen menettelyissä on havaittu puutteita.

3.3.4 Monitorointi

Virtuaalivaluuttatransaktioiden luonteen vuoksi Fiva on suosittanut, että VASP:eilla olisi käytössään tietojärjestelmäpohjainen monitorointijärjestelmä, jotta niillä on tosiasiassa mahdollisuuksia seurata asiakkaan liiketoimia. Erilaiset lohkoketjuanalyysiohjelmat ovat olennainen osa varojen liikkeiden seuraamisessa sekä sen selvittämisessä, mistä varat ovat peräisin ja minne ne ovat mahdollisesti menossa. Lähes kaikilla RA-tiedonkeruulla raportoineilla VASP:eilla on käytössään ulkopuolisen palveluntarjoajan analyysiohjelmisto transaktioiden seurantaa varten ja osa on kehittänyt myös omia analyysiohjelmia. Hälyttävää on se, että jatkuvassa seurannassa osalla VASP:sta on käytössään vain muutama skenaario, jonka perusteella ne seuraavat asiakkaiden toimintaa ja maksuliikennettä. Vaihtelevuutta on myös siinä, kuinka nopeasti monitoroinnin tuottamiin hälytyksiin reagoidaan. Valtaosa VASP:sta tekee todella vähän epäilyttäviä liiketoimia koskevia ilmoituksia rahanpesun selvittelykeskukselle.

4 Valvonnan kohdentaminen

Finanssivalvonta julkaisi vuoden 2022 ominaisriskiarviossa arvionsa kunkin sen valvoman sektorin merkittävyydestä rahanpesun ja terrorismin rahoittamisen torjunnassa samalla neliportaisella asteikolla, jota sektorikohtaisissa riskiarvioissa on käytetty. Virtuaalivaluuttoihin liittyviä palveluita tarjoavat luokiteltiin merkittäväksi (3) sektoriksi, kun otettiin huomioon sektorin ominaisriski ja asiakkaiden määrä. Vuoden 2024 aikana sektorille kohdennettiin kaksi tarkastusta.

MiCA-asetuksen voimaantulon myötä Finanssivalvonnan rekisteriin merkittyjen VASP:ien tulee hakea kryptovarapalvelun tarjoajan toimilupaa, mikäli ne aikovat jatkaa palveluiden tarjoamista. Kryptovarapalvelun tarjoajan toimiluvan edellytyksenä on rahanpesun ja terrorismin rahoittamisen estämistä koskevan sääntelyn asettamien velvoitteiden noudattaminen. Näin ollen toimilupaprosessissa tullaan yksityiskohtaisesti käymään läpi kaikkien toimilupaa hakevien rahanpesun ja terrorismin rahoittamisen estämistä koskevat toimintaperiaatteet, menettelytavat ja sisäinen valvonta kiinnittäen erityistä huomiota riskiarviota laadittaessa havaittuihin puutteisiin.