26/02/2025
ESMA75-223375936-6132

Ohjeet

muiden kryptovarojen kuin omaisuusreferenssitokenien ja sähkörahatokenien tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden järjestelmien ja suojattua pääsyä koskevien protokollien ylläpitämistä koskevien unionin standardien täsmentämisestä

Sisällysluettelo

1 Soveltamisala 2

2 Lainsäädäntöviittaukset, lyhenteet ja määritelmät 3

2.1 Lainsäädäntöviittaukset 3

2.2 Lyhenteet 3

2.3 Määritelmät 4

3 Tarkoitus 4

4 Noudattamista ja ilmoittamista koskevat velvoitteet 5

4.1 Ohjeiden asema 5

4.2 Ilmoittamista koskevat vaatimukset 5

5 Ohjeet, joissa täsmennetään muiden kryptovarojen kuin omaisuusreferenssitokenien ja sähkörahatokenien tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden järjestelmien ja suojattua pääsyä koskevien protokollien ylläpitämistä koskevat unionin standardit 6

5.1 Ohje 1: Yleinen suhteellisuusperiaate 6

5.2 Ohje 2: Järjestelmiä ja suojattua pääsyä koskevia protokollia koskevat hallinnolliset järjestelyt 6

5.3 Ohje 3: Fyysistä suojattua pääsyä koskevat protokollat 7

5.4 Ohje 4: Verkko- ja tietojärjestelmien suojattua pääsyä koskevat protokollat 8

5.5 Ohje 5: Salausavainten hallinta 9

1 Soveltamisala

Kenelle?

1. Ohjeita sovelletaan toimivaltaisiin viranomaisiin ja MiCA-asetuksen 3 artiklan 1 kohdan 13 alakohdassa määriteltyihin ’tarjoajiin’ sekä muiden kryptovarojen kuin omaisuusreferenssitokenien ja sähkörahatokenien kaupankäynnin kohteeksi ottamista hakeviin henkilöihin.

Mitä?

2. Ohjeita sovelletaan MiCA-asetuksen 14 artiklan 1 kohdan d alakohdan osalta.

Milloin?

3. Ohjeita aletaan soveltaa 60 kalenteripäivän kuluttua siitä päivästä, kun ne on julkaistu ESMAn verkkosivustolla kaikilla EU:n virallisilla kielillä.

2 Lainsäädäntöviittaukset, lyhenteet ja määritelmät

2.1 Lainsäädäntöviittaukset

DORA-asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta[1]
ESMA-asetus	Euroopan parlamentin ja neuvoston asetus (EU) N:o 1095/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan arvopaperimarkkinaviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/77/EY kumoamisesta[2]
MiCA-asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2023/1114, annettu 31 päivänä toukokuuta 2023, kryptovarojen markkinoista sekä asetusten (EU) N:o 1093/2010 ja (EU) N:o 1095/2010 ja direktiivien 2013/36/EU ja (EU) 2019/1937 muuttamisesta[3]
NIS 2 - direktiivi	Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta[4]

2.2 Lyhenteet

ART	omaisuusreferenssitoken
EK	Euroopan komissio
EMT	sähkörahatoken
ESMA	Euroopan arvopaperimarkkinaviranomainen
EU	Euroopan unioni

[1] EUVL L 333, 14.12.2022, s. 1–79.
[2] EUVL L 331, 15.12.2010, s. 84.
[3] EUVL L 150, 9.6.2023, s. 40.
[4] EUVL L 333, 12.12.2022, s. 80–133.

2.3 Määritelmät

pääsynvalvonta	tarkoittaa keinoja, joilla varmistetaan, että fyysinen ja looginen pääsy TVT-omaisuuteen sallitaan ja sitä rajoitetaan liiketoiminta- ja tietoturvavaatimusten perusteella[5]
tarjoajat ja kaupankäynnin kohteeksi ottamista hakevat henkilöt	on näissä ohjeissa käytettävä lyhennetty muoto ’muiden kryptovarojen kuin omaisuusreferenssitokenien ja sähkörahatokenien tarjoajista ja kaupankäynnin kohteeksi ottamista hakevista henkilöistä’.
TVT-omaisuus	tarkoittaa DORA-asetuksen 3 artiklan 7 alakohdassa määriteltyä ’TVT-omaisuutta’
TVT-riski	tarkoittaa DORA-asetuksen 3 artiklan 5 alakohdassa määriteltyä ’TVT-riskiä’
verkko- ja tietojärjestelmä	tarkoittaa NIS 2 -direktiivin 6 artiklan 1 alakohdassa määriteltyä ’verkko- ja tietojärjestelmää’

3 Tarkoitus

4. Ohjeet on laadittu yhteistyössä Euroopan pankkiviranomaisen kanssa, ja ne perustuvat MiCA-asetuksen 14 artiklan 1 kohdan d alakohtaan. Ohjeiden tarkoituksena on täsmentää tarjoajia ja kaupankäynnin kohteeksi ottamista hakevia henkilöitä koskevat asianmukaiset unionin standardit, jotka koskevat järjestelmien ja suojattua pääsyä koskevien protokollien ylläpitoa, myös toimintaperiaatteita ja menettelyjä. Ohjeiden tarkoituksena on myös auttaa yhdenmukaistamaan tarjoajiin ja kaupankäynnin kohteeksi ottamista hakeviin henkilöihin sovellettavien MiCA-asetuksen säännösten tulkintaa ja soveltamista.

[5] *ISO/IEC 29146:2016 Information technology — Security techniques — A framework for access management*. Kansainvälinen standardointijärjestö, 2016.

4 Noudattamista ja ilmoittamista koskevat velvoitteet

4.1 Ohjeiden asema

5. ESMA-asetuksen 16 artiklan mukaisesti toimivaltaisten viranomaisten on pyrittävä kaikin tavoin valvomaan näiden ohjeiden täytäntöönpanoa, ja tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi pyrkiä kaikin tavoin noudattamaan niitä.

6. Toimivaltaisten viranomaisten, joihin ohjeita sovelletaan, tulisi asettaa ne soveltuvin osin osaksi kansallista lainsäädäntö- ja/tai valvontakehystään myös silloin, kun tietyt ohjeet on suunnattu ensisijaisesti kryptovaramarkkinoiden toimijoille niiden lainkäyttöalueilla. Tässä tapauksessa toimivaltaisten viranomaisten on valvottava, että finanssimarkkinoiden toimijat noudattavat ohjeita.

4.2 Ilmoittamista koskevat vaatimukset

7. Kahden kuukauden kuluessa siitä päivästä, kun ohjeet on julkaistu ESMAn verkkosivustolla kaikilla EU:n virallisilla kielillä, toimivaltaisten viranomaisten, joihin näitä ohjeita sovelletaan, on ilmoitettava ESMAlle, että ne i) noudattavat tai ii) eivät noudata, mutta aikovat noudattaa tai iii) eivät noudata eivätkä aio noudattaa näitä ohjeita.

8. Noudattamatta jättämisen tapauksessa toimivaltaisten viranomaisten on lisäksi ilmoitettava ESMAlle syynsä näiden ohjeiden noudattamatta jättämiselle kahden kuukauden kuluessa siitä päivästä, kun ohjeet on julkaistu ESMAn verkkosivustolla EU:n kaikilla virallisilla kielillä.

9. ESMAn verkkosivustolla on mallipohja ilmoituksia varten. Kun mallipohja on täytetty, se on lähetettävä ESMAlle.

10. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden ei tarvitse ilmoittaa, noudattavatko ne näitä ohjeita.

5 Ohjeet, joissa täsmennetään muiden kryptovarojen kuin omaisuusreferenssitokenien ja sähkörahatokenien tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden järjestelmien ja suojattua pääsyä koskevien protokollien ylläpitämistä koskevat unionin standardit

5.1 Ohje 1: Yleinen suhteellisuusperiaate

11. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden odotetaan pyrkivän kaikin tavoin noudattamaan näitä ohjeita tavalla, joka on oikeassa suhteessa organisaation kokoon, sen kokonaisriskiprofiiliin sekä sen toiminnan tai operaatioiden luonteeseen, laajuuteen ja monimutkaisuuteen ja jossa otetaan huomioon nämä tekijät.

5.2 Ohje 2: Järjestelmiä ja suojattua pääsyä koskevia protokollia koskevat hallinnolliset järjestelyt

Hallinnolliset järjestelyt

12. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön olisi varmistettava, että sen verkko- ja tietojärjestelmien ylläpitoa ja TVT-riskien lieventämistä varten on olemassa riittävä sisäinen hallinto- ja valvontakehys. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön tulisi myös laatia selkeät tehtävät ja vastuualueet TVT-riskien hallinnasta vastaaville toiminnoille.

13. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön olisi huolehdittava jatkuvasti siitä, että sen henkilöstön taidot ja talousarvioresurssit ovat riittävät TVT-riskien hallintajärjestelyjen tukemiseksi, erityisesti niiden henkilöiden osalta, jotka vastaavat verkko- ja tietojärjestelmien ylläpidosta ja pääsynvalvonnasta. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön tulisi myös huolehtia siitä, että asianomaiset työntekijät, myös kaikki keskeisten tehtävien hoitajat, saavat säännöllisesti asianmukaista koulutusta TVT-riskeistä.

14. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön ylimmän hallintoelimen tulisi olla vastuuvelvollinen organisaation TVT-riskien hallintajärjestelyjen laatimisesta, hyväksymisestä ja täytäntöönpanon valvonnasta, myös siltä osin kuin se liittyy organisaation verkko- ja tietojärjestelmiin ja pääsynvalvontaan.

Tehtävät ja vastuualueet

15. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön tulisi nimetä henkilöstö, joka on organisaatiossa vastuussa TVT-riskien asianmukaisesta

tunnistamisesta, hallinnasta ja valvonnasta. Sen tulisi varmistaa, että TVT-riskien hallinnasta ja turvatoimista vastaavalla henkilöstöllä on asianmukaiset järjestelyt näiden TVT-riskien tunnistamiseksi, seuraamiseksi, arvioimiseksi ja niistä raportoimiseksi.

16. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön tulisi huolehtia siitä, että verkko- ja tietojärjestelmiin ja pääsynvalvontaan liittyvien TVT-riskien hallinnasta vastaava henkilöstö pystyy varmistamaan, että tunnistettuja TVT-riskejä seurataan ja arvioidaan ja niistä raportoidaan ylimmälle hallintoelimelle.

17. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön tulisi määritellä ja jakaa keskeiset tehtävät ja vastuualueet, jotta voidaan luoda järjestelyt, joilla

    i. tunnistetaan ja arvioidaan TVT-riskit, myös palveluntarjoajina olevien kolmansien osapuolten tarjoamiin TVT-palveluihin liittyvät riskit, joille organisaatio altistuu

    ii. määritellään lieventämistoimenpiteet, myös valvontatoimet, joilla lievennetään kolmansien osapuolten TVT-riskejä

    iii. valvotaan ii alakohdassa tarkoitettujen toimenpiteiden vaikuttavuutta ja ryhdytään tarvittaessa toimiin niiden korjaamiseksi

    iv. raportoidaan ylimmälle hallintoelimelle TVT-riskeistä ja lieventämistoimenpiteistä

    v. määritetään ja arvioidaan, aiheutuuko (myös kolmansien osapuolten tarjoamissa) verkko- ja tietojärjestelmissä tai TVT-palveluissa tapahtuneista merkittävistä muutoksista tai merkittävien operatiivisten tai turvallisuuteen liittyvien poikkeamien jälkeen TVT-riskejä

    vi. hallitaan salausavaimia niiden koko elinkaaren ajan.

5.3 Ohje 3: Fyysistä suojattua pääsyä koskevat protokollat

18. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi määritellä fyysiset suojatoimenpiteet tilojensa, tietokeskustensa ja arkaluonteisten alueidensa suojaamiseksi luvattomalta pääsyltä ja ympäristövaaroilta, dokumentoitava kyseiset toimenpiteet ja pantava ne täytäntöön. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön tulisi pitää kirjaa jokaisesta käynnistä tiloissa, joihin pääsy edellyttää lupaa.

19. Fyysinen pääsy verkko- ja tietojärjestelmiin tulisi sallia vain valtuutetuille henkilöille tiedonsaantitarpeen ja pienimmän valtuuden periaatteiden mukaisesti sekä tapauskohtaisesti. Lupa tulisi antaa valtuutetun henkilön tehtävien ja vastuualueiden

perusteella ja rajattava henkilöihin, jotka ovat saaneet asianmukaisen koulutuksen ja joita valvotaan asianmukaisesti. Fyysiset pääsyoikeudet olisi tarkistettava määräajoin ja peruutettava, kun niitä ei enää tarvita.

20. Ympäristövaaroilta suojautumista koskevien asianmukaisten toimenpiteiden tulisi olla oikeassa suhteessa rakennusten merkitykseen sekä niissä sijaitsevien toimintojen tai verkko- ja tietojärjestelmien kriittisyyteen.

5.4 Ohje 4: Verkko- ja tietojärjestelmien suojattua pääsyä koskevat protokollat

21. Looginen pääsy verkko- ja tietojärjestelmiin tulisi rajoittaa tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön nimeämiin valtuutettuihin henkilöihin. Lupa tulisi antaa henkilön tehtävien ja vastuualueiden perusteella ja rajattava henkilöihin, jotka ovat saaneet asianmukaisen koulutuksen ja joiden pääsyä järjestelmiin valvotaan. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi ottaa käyttöön valvontatoimet, joilla tällainen pääsy verkko- ja tietojärjestelmiin rajoitetaan luotettavasti niihin, joilla on siihen oikeutettu liiketoimintaan perustuva tarve. Sähköinen pääsy tietoihin ja järjestelmiin sovellusten avulla tulisi rajata vähimpään, mikä on tarpeen asiaankuuluvan palvelun tarjoamiseksi.

22. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi ottaa käyttöön tehokkaat valvontakeinot etuoikeutetun järjestelmään pääsyn osalta rajoittamalla ja valvomalla tiukasti henkilöstöä, jolla on laajat pääsyoikeudet järjestelmään. Käyttöön otettavia valvontatoimia ovat muun muassa tehtäväperusteinen pääsyoikeus, etuoikeutettujen käyttäjien verkko- ja tietojärjestelmässä tekemien toimien kirjaaminen ja tarkastelu, vahva todennus ja poikkeamien seuranta. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön tulisi hallinnoida tieto-omaisuuden ja sitä tukevien järjestelmien pääsyoikeuksia tiedonsaantitarpeen ja pienimmän valtuuden periaatteen perusteella. Loogiset pääsyoikeudet tulisi tarkistaa määräajoin ja peruutettava, kun niitä ei enää tarvita.

23. Kulkulokeja tulisi säilyttää niin kauan kuin määritettyjen liiketoimintojen, tukiprosessien ja tieto-omaisuuden kriittisyys sitä edellyttää, sanotun kuitenkaan rajoittamatta EU:n ja kansallisessa lainsäädännössä asetettuja säilytysvaatimuksia. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi näiden tietojen avulla helpottaa palvelujensa tarjoamisen yhteydessä havaittujen poikkeavien toimintojen tunnistamista ja tutkimista.

24. Hallinnollinen etäpääsy kriittiseen TVT-omaisuuteen tulisi myöntää vain tiedonsaantitarpeen ja pienimmän valtuuden periaatteen perusteella ja vain, kun käytettävissä on vahvoja todentamisratkaisuja.

25. Näiden pääsynvalvontaprosessien vaarantuminen tai kiertäminen tulisi pystyä estämään käyttämällä pääsynvalvontaprosesseihin liittyviä tuotteita, työkaluja ja menettelyjä. Tähän sisältyy vastaavien tuotteiden, työkalujen ja menettelyjen käyttöönotto, toimittaminen, peruuttaminen ja poistaminen.

5.5 Ohje 5: Salausavainten hallinta

26. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevan henkilön tulisi huolehtia salausavainten hallinnasta osana TVT-riskien osalta avainhenkilöille osoitettuja tehtäviä ja vastuualueita. Tarjoajan tai kaupankäynnin kohteeksi ottamista hakevien henkilöiden henkilöstön tulisi huolehtia salausavainten hallinnasta koko niiden elinkaaren ajan, muun muassa avainten tuottamisesta, uusimisesta, tallentamisesta, varmuuskopioinnista, arkistoinnista, palauttamisesta, siirtämisestä, käytöstä poistamisesta, peruuttamisesta ja tuhoamisesta.

27. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi määritellä ja toteuttaa valvontatoimenpiteitä, joilla salausavaimia suojataan koko niiden elinkaaren ajan katoamiselta, luvattomalta käytöltä, paljastamiselta ja muuttamiselta.

28. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi kehittää ja ottaa käyttöön menetelmiä salausavainten korvaamiseksi, jos avaimia katoaa, vaarantuu tai vahingoittuu.

29. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi perustaa rekisteri kaikista varmenteista ja varmenteiden tallennuslaitteista ainakin kriittisen TVT-omaisuuden osalta ja pidettävä sitä yllä. Rekisteri tulisi pitää ajan tasalla.

30. Tarjoajien ja kaupankäynnin kohteeksi ottamista hakevien henkilöiden tulisi huolehtia varmenteiden nopeasta uusimisesta ennen niiden voimassaolon päättymistä.