Liikenne- ja viestintävirasto

Ohje

215/2019 O
9.10.2019

Hyväksytyn eIDAS-luottamuspalvelun arviointi-kertomus

Liikenne- ja viestintäviraston ohje

215/2019 O

Sisältö

1 Johdanto 2

1.1 Ohjeen tarkoitus 2

1.2 Ohjeen voimaantulo 2

1.3 Säädökset, määritelmät ja lyhenteet 3

2 Vaatimustenmukaisuuden arviointikertomuksen toimittaminen 4

3 Luotettu luettelo (trusted list) 5

4 Arviointikertomuksen sisältö 6

4.1 Vaatimuksenmukaisuuden arviointilaitosta koskevat perustiedot 6

4.2 Perustiedot arvioitavasta luottamuspalvelusta 6

4.3 Perustiedot vaatimuksenmukaisuuden arvioinnin toteuttamisesta 7

4.4 Vaatimustenmukaisuuden osoittaminen 8

4.4.1 Palveluntarjoajaa koskevat erityisvaatimukset 8

4.4.2 Hyväksyttyä luottamuspalvelua koskevat erityisvaatimukset 8

4.5 Poikkeamien raportointi 9

1 Johdanto

1.1 Ohjeen tarkoitus

Ohje koskee eIDAS-asetuksen mukaisia hyväksyttyjä luottamuspalveluita.

Ohje on tarkoitettu akkreditoiduille vaatimustenmukaisuuden arviointilaitoksille, jotka tarkastavat hyväksytyn luottamuspalvelun tarjoajan ja hyväksytyn luottamuspalvelun vaatimustenmukaisuuden. Ohje kuvaa arvioinnin lopputuloksena annettavien arviointikertomusten vähimmäissisältöä ja esittämistapaa.

Liikenne- ja viestintävirastolle toimitettavista ilmoituksista on julkaistu erillinen ohje (214/2016 O).

Liikenne- ja viestintäviraston tehtävänä on valvoa tunnistus- ja luottamuspalvelulain (617/2009) 42 §:n nojalla lain ja EU:n eIDAS-asetuksen noudattamista. Tämä ohje on annettu lain 42 §:n yleisen valtuuden nojalla.

1.2 Ohjeen voimaantulo

Ohje 215/2019 O tulee voimaan 9.10.2019

Ohje on voimassa toistaiseksi ja sitä täydennetään ja muutetaan tarvittaessa. Tällöin ohjeen numero 215 säilyy, mutta päivämäärä vaihtuu ja vuosiluku vaihtuu tarvittaessa. Ohjeen muutetut versiot listataan seuraavaan taulukkoon

Voimassa oleva ohje julkaistaan Liikenne- ja viestintäviraston verkkosivulla https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen ja https://www.traficom.fi/fi/saadokset

Versio	Päiväys	Kuvaus/muutos	Tekijä
215/2019 O Hyväksytyn luottamuspalvelun arviointikertomus	9.10.2019	2. julkaistu versio ▪ Tunnistuspalvelun tarkastuskertomusta koskeva osuus on siirretty ohjeeseen 211/2019 O ▪ Ohjeeseen on tehty teknisluonteisia tekstimuutoksia mm. viranomaisen nimenmuutoksen takia ja otsikointia on korjattu.	Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus
215/2016 O Tunnistus- ja luottamuspalveluiden arviointikertomukset	2.11.2016	1. julkaistu versio	Viestintävirasto, Kyberturvallisuuskeskus

1.3 Säädökset, määritelmät ja lyhenteet

eIDAS: Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta.

Tunnistus- ja luottamuspalvelulaki: laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009 muutoksineen)

Hyväksytyn luottamuspalvelun tarjoaja (QTSP, qualified trusted service provider):

> ***eIDAS artikla 3 Määritelmät***
>
> *20) 'hyväksytyllä luottamuspalvelun tarjoajalla' luottamuspalvelun tarjoajaa, joka tarjoaa yhtä tai useampaa hyväksyttyä luottamuspalvelua ja jolle valvontaelin on myöntänyt hyväksytyn aseman;*

Hyväksytty luottamuspalvelu (QTS, qualified trusted service):

> **eIDAS artikla 3 Määritelmät**
>
> *16) 'luottamuspalvelulla' sähköistä palvelua, jota yleensä tarjotaan vastiketta vastaan ja joka koostuu seuraavista:*
>
> *a) sähköisten allekirjoitusten, sähköisten leimojen tai sähköisten aikaleimojen, sähköisten rekisteröityjen jakelupalvelujen ja kyseisiin palveluihin liittyvien varmenteiden luomisesta, tarkastamisesta ja validoinnista; tai*
>
> *b) verkkosivustojen todentamisen varmenteiden luomisesta, tarkastamisesta ja validoinnista; tai*
>
> *c) sähköisten allekirjoitusten, leimojen tai kyseisiin palveluihin liittyvien varmenteiden säilyttämisestä;*
>
> *17) 'hyväksytyllä luottamuspalvelulla' luottamuspalvelua, joka täyttää tässä asetuksessa säädetyt sovellettavat vaatimukset;*

Vaatimustenmukaisuuden arviointilaitos (CAB, conformity assessment body):

> ***eIDAS artikla 3 Määritelmät***
>
> *18) 'vaatimustenmukaisuuden arviointilaitoksella' asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa määriteltyä elintä, joka on akkreditoitu kyseisen asetuksen mukaisesti päteväksi arvioimaan hyväksyttyjen luottamuspalvelun tarjoajien ja niiden tarjoamien hyväksyttyjen luottamuspalvelujen vaatimustenmukaisuus;*

Vaatimustenmukaisuuden arviointikertomus (CAR, conformity assessment report):

> **Ks. eIDAS artikla 20 Hyväksyttyjen luottamuspalvelun tarjoajien valvonta**
>
> 1. Vaatimustenmukaisuuden arviointilaitoksen on tarkastettava hyväksytyt luottamuspalvelun tarjoajat […]. Tarkastuksen tarkoituksena on vahvistaa, että hyväksytyt luottamuspalvelun tarjoajat ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset. Hyväksyttyjen luottamuspalvelun tarjoajien on toimitettava tarkastuksen perusteella laadittava vaatimustenmukaisuuden arviointikertomus valvontaelimelle […].
>
> […]
>
> **Ks. eIDAS 21 artikla Hyväksytyn luottamuspalvelun aloittaminen**
>
> 1. Jos luottamuspalvelun tarjoajat, joilla ei ole hyväksyttyä asemaa, aikovat tarjota hyväksyttyjä luottamuspalveluja, niiden on toimitettava valvontaelimelle ilmoitus aikomuksestaan yhdessä vaatimustenmukaisuuden arviointilaitoksen myöntämän vaatimustenmukaisuuden arviointikertomuksen kanssa.
>
> […]

2 Vaatimustenmukaisuuden arviointikertomuksen toimittaminen

Arviointikertomus on toimitettava Liikenne- ja viestintävirastolle:

1. ennen toiminnan aloittamista, jos luottamuspalvelun tarjoajat, joilla ei ole hyväksyttyä asemaa, aikovat tarjota hyväksyttyjä luottamuspalveluja; ja

2. Vähintään 24 kuukauden välein sen jälkeen, kun luottamuspalvelun tarjoaja on toimittanut toiminnan aloittamisen yhteydessä annettavan arviointikertomuksen Liikenne- ja viestintävirastolle.

> ***SÄÄNNÖKSET***
>
> ***eIDAS-asetus 20 artikla Hyväksyttyjen luottamuspalvelun tarjoajien valvonta***
>
> *1. Vaatimustenmukaisuuden arviointilaitoksen on tarkastettava hyväksytyt luottamuspalvelun tarjoajat vähintään 24 kuukauden välein niiden omalla kustannuksella. Tarkastuksen tarkoituksena on vahvistaa, että hyväksytyt luottamuspalvelun tarjoajat ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset. Hyväksyttyjen luottamuspalvelun tarjoajien on toimitettava tarkastuksen perusteella laadittava vaatimustenmukaisuuden arviointikertomus valvontaelimelle kolmen työpäivän kuluessa sen vastaanottamisesta.*
>
> *2. Valvontaelin voi milloin tahansa tehdä hyväksytyille luottamuspalvelun tarjoajille tarkastuksia tai pyytää vaatimustenmukaisuuden arviointilaitosta suorittamaan hyväksyttyjä luottamuspalvelun tarjoajia koskevan vaatimustenmukaisuuden arvioinnin näiden hyväksyttyjen luottamuspalvelun tarjoajien kus-*

tannuksella sen vahvistamiseksi, että ne ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset, sanotun kuitenkaan rajoittamatta 1 kohdan soveltamista. Jos näyttää siltä, että henkilötietojen suojaan liittyviä sääntöjä on rikottu, valvontaelimen on ilmoitettava tarkastustensa tuloksista tietosuojaviranomaisille.

[…]

eIDAS-asetus 21 artikla Hyväksytyn luottamuspalvelun aloittaminen

1. Jos luottamuspalvelun tarjoajat, joilla ei ole hyväksyttyä asemaa, aikovat tarjota hyväksyttyjä luottamuspalveluja, niiden on toimitettava valvontaelimelle ilmoitus aikomuksestaan yhdessä vaatimustenmukaisuuden arviointilaitoksen myöntämän vaatimustenmukaisuuden arviointikertomuksen kanssa.

2. Valvontaelin tarkastaa, täyttävätkö luottamuspalvelun tarjoaja ja sen tarjoamat luottamuspalvelut tässä asetuksessa säädetyt vaatimukset ja erityisesti hyväksyttyjä luottamuspalvelun tarjoajia ja niiden tarjoamia hyväksyttyjä luottamuspalveluja koskevat vaatimukset.

Jos valvontaelin päättää, että luottamuspalvelun tarjoaja ja sen tarjoamat luottamuspalvelut täyttävät ensimmäisessä alakohdassa tarkoitetut vaatimukset, valvontaelimen on myönnettävä luottamuspalvelun tarjoajalle ja sen tarjoamille luottamuspalveluille hyväksytty asema sekä ilmoitettava asiasta 22 artiklan 3 kohdassa tarkoitetulle elimelle 22 artiklan 1 kohdassa tarkoitettujen luotettujen luetteloiden ajan tasalle saattamista varten viimeistään kolmen kuukauden kuluttua tämän artiklan 1 kohdan mukaisesta ilmoituksesta.

Jos tarkastusta ei saada päätökseen kolmen kuukauden kuluessa ilmoituksesta, valvontaelimen on ilmoitettava asiasta luottamuspalvelun tarjoajalle ja yksilöitävä viivästyksen syyt ja ajanjakso, jonka aikana tarkastus on saatava päätökseen.

3. Hyväksytyt luottamuspalvelun tarjoajat voivat ryhtyä tarjoamaan hyväksyttyä luottamuspalvelua sen jälkeen kun hyväksytty asema on merkitty 22 artiklan 1 kohdassa tarkoitettuihin luotettuihin luetteloihin.

[…]

Tunnistus- ja luottamuspalvelulaki 32 §

Vaatimustenmukaisuuden arviointilaitos tarkastaa hyväksytyn luottamuspalvelun tarjoajan ja hyväksytyn luottamuspalvelun vaatimustenmukaisuuden noudattaen, mitä siitä sähköisestä tunnistamisesta ja luottamuspalveluista annetussa EU:n asetuksessa säädetään.

Liikenne- ja viestintäviraston oikeudesta antaa tarkempia määräyksiä vaatimustenmukaisuuden arvioinnissa käytettävistä arviointiperusteista säädetään 42 §:ssä. Liikenne- ja viestintävirasto voi määrätä arviointiperusteeksi Euroopan unionin tai muun kansainvälisen toimielimen antamia säännöksiä tai ohjeita, julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia ohjeita ja yleisesti käytettyjä tietoturvallisuusstandardeja tai menettelyjä.

3 Luotettu luettelo (trusted list)

Jos ilmoitettu palvelu täyttää hyväksytylle luottamuspalvelun tarjoajalle ja hyväksytylle luottamuspalvelulle asetetut vaati-

mukset, Liikenne- ja viestintävirasto myöntää luottamuspalvelun tarjoajalle ja sen tarjoamille luottamuspalveluille hyväksytty asema sekä merkitsee palvelut luotettuun luetteloon.

Suomen luotettu luettelo löytyy verkko-osoitteesta https://dp.trustedlist.fi/fi-tl.pdf

eIDAS 22 artikla Luotetut luettelot

1. Kunkin jäsenvaltion on laadittava, ylläpidettävä ja julkaistava luotettuja luetteloja, jotka sisältävät tietoa niiden vastuulle kuuluvista hyväksytyistä luottamuspalvelun tarjoajista ja niiden tarjoamista hyväksytyistä luottamuspalveluista.

4 Arviointikertomuksen sisältö

Hyväksytyn luottamuspalvelun arviointikertomuksesta tulee käydä ilmi vähintään seuraavat perustiedot.

4.1 Vaatimuksenmukaisuuden arviointilaitosta koskevat perustiedot

1. Yrityksen tai yhteisön nimi ja yksilöivä rekisterinumero tai -tunnus;

2. jos yritys tai yhteisö on sijoittunut muuhun ETA-alueen valtion kuin Suomeen, rekisteri, johon ulkomainen yhteisö tai yritys on merkitty;

3. postiosoite ja yhteyshenkilöt; ja sähköpostiosoitteet Liikenne- ja viestintäviraston tiedusteluja varten.

4.2 Perustiedot arvioitavasta luottamuspalvelusta

4. Arvioitavan hyväksytyn luottamuspalvelun tai hyväksytyn luottamuspalvelun aseman vahvistamista hakevan palvelun nimi/nimet sekä palvelutyypit ilmoitusohjeen 214/2016 O luvun 4.1.1. alakohdan 4 mukaisesti eli:

    a. hyväksytty sähköisen allekirjoituksen varmenne (eIDAS-asetus 28 artikla);

    b. hyväksytty validointipalvelu hyväksytylle sähköiselle allekirjoitukselle (eIDAS-asetus 33 artikla);

    c. hyväksytty säilyttämispalvelu hyväksytylle sähköiselle allekirjoitukselle (eIDAS-asetus 34 artikla);

    d. hyväksytty sähköisen leiman varmenne (eIDAS-asetus 38 artikla);

    e. hyväksytty validointipalvelu hyväksytylle sähköiselle leimalle (eIDAS-asetus 40 artikla);

f. hyväksytty säilyttämispalvelu hyväksytylle sähköiselle leimalle (eIDAS-asetus 40 artikla);

g. hyväksytty sähköinen aikaleima (eIDAS-asetus 42 artikla);

h. hyväksytty sähköinen rekisteröity jakelupalvelu (eIDAS-asetus 44 artikla); tai

i. verkkosivujen todentamisen hyväksytty varmenne (eIDAS-asetus 45 artikla).

4.3 Perustiedot vaatimuksenmukaisuuden arvioinnin toteuttamisesta

5. Kuvaus siitä, minkä osan luottamuspalvelusta arviointi kattaa;

6. selvitys siitä, millaisia menetelmiä arvioinnissa on käytetty eri osa-alueiden arviointiin;

7. tiedot dokumentaatiosta, jota on käytetty vaatimuksenmukaisuuden arvioinnissa; ja

8. arvioinnin suorittamisen ajankohta ja kesto henkilötyöaikana (henkilötyöpäivinä tai tunteina).

Arviointikertomuksessa on kuvattava, minkä/mitä hyväksyttyjä luottamuspalveluja arviointi kattaa sekä kattaako arvio palvelun kokonaan vai osan siitä. Hyväksytyn luottamuspalvelun tarjoaja voi tilata arvioinnin osissa myös kahdelta tai usealta vaatimuksenmukaisuuden arviointilaitokselta. On tärkeää, että arviointikertomuksesta ilmenee yksiselitteisesti, kattaako vaatimuksenmukaisuuden arviointilaitoksen laatima arviointikertomus vain osan kohdan 4.4 vaatimuksista vai kaikki ko. vaatimukset.

Arviointikertomuksesta on käytävä ilmi, millaisia menetelmiä vaatimuksenmukaisuuden arvioinnissa on käytetty. Pelkkää standardilistausta ei voida pitää riittävänä, vaan arviointikertomuksessa on kuvattava, mitä menetelmää kunkin kohdassa 4.4 mainitun osa-alueen arviointiin on käytetty.

Arviointikertomuksessa on listattava, mitä palveluntarjoajan dokumentaatiota on arvioitu. Kaikkea arviointiin liittyvää materiaalia ei ole tarpeen liittää Liikenne- ja viestintävirastolle toimitettavaan arviointikertomukseen. Virasto voi tarvittaessa pyytää toimittamaan tarkemman dokumentaation. Liikenne- ja viestintäviraston tiedonsaantioikeus perustuu tunnistus- ja luottamuspalvelulain 43 §:ään, jonka mukaan virastolla on oikeus salassapitosäännösten estämättä saada tehtäviensä suorittamiseksi tarvittavat tiedot niiltä, joiden oikeuksista ja velvollisuuksista ko. laissa säädetään ja jotka toimivat näiden lukuun.

4.4 Vaatimustenmukaisuuden osoittaminen

Luottamuspalvelun vaatimuksenmukaisuuden arvioinnin tarkoituksena on osoittaa, että Liikenne- ja viestintävirastolle ilmoitettu hyväksytty luottamuspalvelu täyttää eIDAS-asetuksessa säädetyt vaatimukset.

Arviointikertomuksesta tulee käydä ilmi, miten seuraavien vaatimusten täyttyminen on arvioitu ja millä perusteella luottamuspalvelun arvioidaan täyttävän seuraavat vaatimukset:

4.4.1 Palveluntarjoajaa koskevat erityisvaatimukset

9. Tietojen käsittelyä ja suojaamista koskevat vaatimukset (eIDAS-asetus 5 art);

10. Vastuuta ja todistustaakkaa koskevat säännökset (eIDAS-asetus 13 art, kohdat 1-2 ja tunnistus- ja luottamuspalvelulaki 41 §);

11. Esteettömyyttä vammaisten näkökulmasta koskevat vaatimukset (eIDAS-asetus 15 art);

12. Luottamuspalvelun tarjoajiin sovellettavat tietoturvavaatimukset (eIDAS-asetus 19 art, kohta 1); ja

13. Hyväksyttyjä luottamuspalvelun tarjoajia koskevat vaatimukset (eIDAS-asetus art 24, kohta 2, pl. 2 k).

4.4.2 Hyväksyttyä luottamuspalvelua koskevat erityisvaatimukset

14. Määräys 72, 20–21 §:n mukaiset luottamuspalvelun yleiset arviointikriteerit;

15. Hyväksyttyä varmennetta koskevat vaatimukset (eIDAS-asetus 24 art, alakohdat 1 a-d, 2 k ja 3-4);

16. Sähköisten allekirjoitusten hyväksyttyjä varmenteita koskevat vaatimukset (eIDAS-asetus 28 art, kohta 1);

17. Hyväksyttyjen sähköisten allekirjoitusten hyväksyttyjä validointipalveluja koskevat vaatimukset (eIDAS-asetus 32 ja 33 art);

18. Hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä säilyttämispalvelua koskevat vaatimukset (eIDAS-asetus 34 art);

19. Sähköisten leimojen hyväksyttyjä varmenteita koskevat vaatimukset (eIDAS-asetus 38 art);

20. Hyväksyttyjen sähköisten leimojen hyväksyttyä validointipalvelua koskevat vaatimukset (eIDAS-asetus 40, 32 ja 33 artiklat);

21. Hyväksyttyjen sähköisten leimojen hyväksyttyä säilyttämispalvelua koskevat vaatimukset (eIDAS-asetus 40 ja 34 artiklat);

22. Hyväksyttyjä sähköisiä aikaleimoja koskevat vaatimukset (eIDAS-asetus 42 art);

23. Hyväksyttyjä sähköisiä rekisteröityjä jakelupalveluja koskevat vaatimukset (eIDAS-asetus 44 art); ja

24. Verkkosivustojen todentamisen hyväksyttyjä varmenteita koskevat vaatimukset (eIDAS-asetus 45 art).

4.5 Poikkeamien raportointi

Vaatimuksenmukaisuuden arvioinnin yhteydessä löytyy tyypillisesti poikkeamia, joita korjataan arvioinnin aikana tai pian sen jälkeen. Normaalitilanteessa havaitut poikkeamat on korjattu ennen arviointikertomuksen toimittamista Liikenne- ja viestintävirastolle.

Jos poikkeamia kuitenkin jää, niiden on käytävä yksiselitteisesti ilmi arviointikertomuksesta. Tällöin arviointikertomukseen on liitettävä tieto siitä, mitä vähäisiä tai muita poikkeamia järjestelmään on jätetty ja millä aikataululla ja miten ne tullaan korjaamaan. Virasto ei laadi poikkeamien vakavuusasteikkoa, vaan niiden arviointi jää arviointi- ja ilmoitusvaiheessa luottamuspalveluntarjoajan ja arvioijan välisen harkinnan varaan. Virasto tekee lopullisen arvion siitä, mitä poikkeamia hyväksytään. Tarvittaessa Liikenne- ja viestintävirasto edellyttää korjaamaan havaitut poikkeamat.