KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2015/1502,

annettu 8 päivänä syyskuuta 2015,

teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta 23 päivänä heinäkuuta 2014 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 ([1]) ja erityisesti sen 8 artiklan 3 kohdan,

sekä katsoo seuraavaa:

(1) Asetuksen (EU) N:o 910/2014 8 artiklassa säädetään, että 9 artiklan 1 kohdan nojalla ilmoitetussa sähköisen tunnistamisen järjestelmässä on kyseisen järjestelmän puitteissa myönnettyjen sähköisen tunnistamisen menetelmien osalta määritettävä matala, korotettu ja korkea varmuustaso.

(2) On olennaisen tärkeää määrittää tekniset vähimmäiseritelmät, -standardit ja -menettelyt, jotta voidaan varmistaa yhteisymmärrys varmuustasojen yksityiskohdista ja yhteentoimivuus ilmoitettujen sähköisen tunnistamisen järjestelmien kansallisten varmuustasojen kartoittamisessa suhteessa 8 artiklan mukaisiin varmuustasoihin asetuksen (EU) N:o 910/2014 12 artiklan 4 kohdan b alakohdassa säädetyllä tavalla.

(3) Kansainvälinen ISO/IEC 29115 -standardi on otettu huomioon tässä täytäntöönpanosäädöksessä vahvistettuja eritelmiä ja menettelyjä varten ensisijaisena kansainvälisenä standardina, joka on sovellettavissa sähköisen tunnistamisen menetelmien varmuustasojen alalla. Asetuksen (EU) N:o 910/2014 sisältö poikkeaa kuitenkin tästä kansainvälisestä standardista erityisesti henkilöllisyyden todistamista ja varmentamista koskevien vaatimusten osalta sekä siinä, miten jäsenvaltioissa käytettävien identiteetin hallintajärjestelmien ja EU:ssa samaan tarkoituksen käytössä olevien välineiden väliset erot otetaan huomioon. Tämän vuoksi liitteessä ei pitäisi viitata ISO/IEC 29115 -standardin konkreettiseen sisältöön, vaikka liite perustuu kyseiseen kansainväliseen standardiin.

(4) Tämä asetus on laadittu käyttämällä tuloksiin perustuvaa tarkoituksenmukaisinta lähestymistapaa, mikä näkyy myös käytetyissä termien ja käsitteiden määritelmissä. Niissä otetaan huomioon asetuksen (EU) N:o 910/2014 tavoite liittyen sähköisen tunnistamisen menetelmien varmuustasoihin. Tämän vuoksi laajamittainen STORK-pilottihanke ja siinä laaditut eritelmät sekä ISO/IEC 29115 -standardin määritelmät ja käsitteet olisi otettava mahdollisimman pitkälti huomioon tässä täytäntöönpanosäädöksessä vahvistettavissa eritelmissä ja menettelyissä.

(5) Riippuen asiayhteydestä, jossa henkilöllisyyden todistamiseen liittyvä näkökohta on varmennettava, luotettava lähde voi olla erityyppinen, esimerkiksi rekisteri, asiakirja tai elin. Luotettavat lähteet voivat olla erilaisia eri jäsenvaltioissa jopa samanlaisessa asiayhteydessä.

(6) Henkilöllisyyden todistamista ja varmentamista koskevissa vaatimuksissa olisi otettava huomioon eri järjestelmät ja käytännöt ja samalla varmistettava riittävän suuri varmuus, jotta voidaan luoda tarvittava luottamus. Sen vuoksi menettelyjä, joita on käytetty aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen, olisi voitava hyväksyä ainoastaan varmistuttaessa siitä, että kyseiset menettelyt täyttävät vastaavaa varmuustasoa varten vahvistetut vaatimukset.

([1]) EUVL L 257, 28.8.2014, s. 73.

(7) Yleensä käytetään tiettyjä todentamistekijöitä, kuten yhteisesti salattuja tietoja, fyysisiä laitteita ja fyysisiä ominaisuuksia. Todentamistekijöiden lisäämistä etenkin muista tekijöiden luokista olisi kannustettava, jotta voidaan parantaa todentamismenettelyn turvallisuutta.

(8) Tämä asetus ei saisi vaikuttaa oikeushenkilöiden edustamisoikeuksiin. Liitteessä olisi kuitenkin vahvistettava vaatimukset luonnollisten ja oikeushenkilöiden sähköisen tunnistamisen menetelmien välisestä kytköksestä.

(9) Olisi tunnustettava tietoturvallisuus- ja palvelunhallintajärjestelmien tärkeys sekä se, että on tärkeää käyttää hyväksyttyjä menetelmiä ja soveltaa standardien, kuten sarjojen ISO/IEC 27000 ja ISO/IEC 20000 standardien, periaatteita.

(10) Varmuustasoihin liittyvät jäsenvaltioiden hyvät käytännöt olisi myös otettava huomioon.

(11) Kansainvälisiin standardeihin perustuva tietotekninen tietoturvasertifiointi on tärkeä väline tarkastettaessa, vastaavatko tuotteet turvallisuudeltaan tämän täytäntöönpanosäädöksen vaatimuksia.

(12) Asetuksen (EY) N:o 910/2014 48 artiklassa tarkoitettu komitea ei antanut lausuntoa puheenjohtajansa asettamassa määräajassa,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

1. Ilmoitetun sähköisen tunnistamisen järjestelmän puitteissa myönnettyjen sähköisen tunnistamisen menetelmien matala, korotettu ja korkea varmuustaso on määritettävä käyttäen liitteessä esitettyjä eritelmiä ja menettelyjä.

2. Liitteessä esitettyjä eritelmiä ja menettelyjä on käytettävä ilmoitetun sähköisen tunnistamisen järjestelmän puitteissa myönnettyjen sähköisen tunnistamisen menetelmien varmuustason täsmentämiseksi määrittämällä seuraavien osatekijöiden luotettavuus ja laatu:

a) rekisteröinti, joka määritellään tämän asetuksen liitteessä olevassa 2.1 kohdassa asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan a alakohdan mukaisesti;

b) sähköisen tunnistamisen menetelmien hallinta, joka määritellään tämän asetuksen liitteessä olevassa 2.2 kohdassa asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan b ja f alakohdan mukaisesti;

c) todentaminen, joka määritellään tämän asetuksen liitteessä olevassa 2.3 kohdassa asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan c alakohdan mukaisesti;

d) hallinnointi ja organisointi, jotka määritellään tämän asetuksen liitteessä olevassa 2.4 kohdassa asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan d ja e alakohdan mukaisesti.

3. Jos ilmoitetun sähköisen tunnistamisen järjestelmän puitteissa myönnetty sähköisen tunnistamisen menetelmä täyttää vaatimuksen korkeammalla varmuustasolla, sen katsotaan täyttävän vastaavan vaatimuksen myös matalammalla varmuustasolla.

4. Jollei liitteen asianomaisessa osassa toisin mainita, kaikki osatekijät, jotka liitteessä luetellaan ilmoitetun sähköisen tunnistamisen järjestelmän puitteissa myönnetyn sähköisen tunnistamisen menetelmän tietyn varmuustason osalta, on täytettävä ilmoitetun varmuustason saavuttamiseksi.

2 artikla

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 8 päivänä syyskuuta 2015.

Komission puolesta

Puheenjohtaja

Jean-Claude JUNCKER

LIITE

Tekniset eritelmät ja menettelyt ilmoitetun sähköisen tunnistamisen järjestelmän puitteissa myönnettyjen sähköisen tunnistamisen menetelmien matalaa, korotettua ja korkeaa varmuustasoa varten

1. Sovellettavat määritelmät

Tässä liitteessä sovelletaan seuraavia määritelmiä:

1) 'luotettavalla lähteellä' tarkoitetaan mitä tahansa sellaista lähdettä muodosta riippumatta, josta voidaan luotettavasti saada paikkansapitäviä tietoja ja/tai todisteita, joita voidaan käyttää henkilöllisyyden todistamiseen;

2) 'todentamistekijällä' tarkoitetaan tekijää, joka on vahvistettu henkilöön kytkeytyväksi ja joka kuuluu johonkin seuraavista luokista:

   a) 'hallussapitoon perustavalla todentamistekijällä' tarkoitetaan todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;

   b) 'tiedossaoloon perustavalla todentamistekijällä' tarkoitetaan todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;

   c) 'luontaisella todentamistekijällä' tarkoitetaan todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen, jonka henkilön on osoitettava fyysiseksi ominaisuudekseen;

3) 'dynaamisella todentamisella' tarkoitetaan sähköistä prosessia, jossa käytetään salausta tai muita tekniikoita, joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa;

4) 'tietoturvallisuuden hallintajärjestelmällä' tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvallisuuteen liittyvät riskit hyväksyttävällä tasolla.

2. Tekniset eritelmät ja menettelyt

Tässä liitteessä esitettyjen teknisten eritelmien ja menettelyjen osatekijöitä käytetään määriteltäessä, miten asetuksen (EU) N:o 910/2014 8 artiklan vaatimuksia ja perusteita on sovellettava sähköisen tunnistamisen järjestelmän puitteissa myönnettyihin sähköisen tunnistamisen menetelmiin.

2.1 *Rekisteröinti*

2.1.1 Hakemus ja rekisteröinti

Varmuustaso	Tarvittavat osatekijät
Matala	1. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmien käyttöön liittyvistä ehdoista ja edellytyksistä. 2. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmiin liittyvistä suositelluista varotoimista. 3. Kerätään asiaankuuluvat tunnistetiedot, jotka tarvitaan henkilöllisyyden todistamista ja varmentamista varten.
Korotettu	Sama kuin tasolla "matala".
Korkea	Sama kuin tasolla "matala".

2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)

Varmuustaso	Tarvittavat osatekijät
Matala	1. Henkilöllä voidaan olettaa olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan. 2. Todisteen voidaan olettaa olevan aito tai luotettavan lähteen mukaan olemassa oleva, ja se näyttää olevan voimassa. 3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.
Korotettu	Sama kuin tasolla ”matala”, minkä lisäksi yhden kohdissa 1–4 mainituista vaihtoehdoista on täytyttävä: 1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan ja todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön ja on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; tai 2. henkilöllisyystodistus esitetään rekisteröintiprosessin aikana siinä jäsenvaltiossa, jossa todistus on myönnetty, ja todistus näyttää liittyvän sen esittäneeseen henkilöön ja on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todistus on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; tai 3. Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät menettelyt tarjoavat vastaavan varmuuden kuin 2.1.2. kohdassa esitetyt menettelyt varmuustasolla ”korotettu”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavantasoisen varmuuden on vahvistanut Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 ([1]) 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin; tai 4. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on ”korotettu” tai ”korkea”, ja ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista, henkilöllisyyden todistamis- ja varmentamismenettelyjä ei tarvitse toistaa. Jos perustana olevaa sähköisen tunnistamisen menetelmää ei ole ilmoitettu, varmuustason ”korotettu” tai ”korkea” on oltava asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen tai vastaavan elimen vahvistama.

Varmuustaso	Tarvittavat osatekijät
Korkea	Joko kohdan 1 tai 2 vaatimusten on täytyttävä: 1. Sama kuin tasolla ”korotettu”, minkä lisäksi yhden kohdissa a–c mainituista vaihtoehdoista on täytyttävä: a) Jos henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä valokuva tai biometrinen tunniste, jossa sähköisen tunnistamisen menetelmää haetaan, ja kyseinen todiste edustaa ilmoitettua henkilöllisyyttä, todiste tarkistetaan sen määrittämiseksi, onko se luotettavan lähteen mukaan voimassa; ja hakijalla todetaan olevan ilmoitettu henkilöllisyys vertaamalla yhtä tai useampaa henkilön fyysistä ominaisuutta luotettavaan lähteeseen; tai b) Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät menettelyt tarjoavat vastaavan varmuuden kuin 2.1.2 kohdassa esitetyt menettelyt varmuustasolla ”korkea”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavantasoisen varmuuden on vahvistanut asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin ja on ryhdytty toimiin sen osoittamiseksi, että aiempien menettelyjen tulokset ovat edelleen voimassa; tai c) Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on ”korkea”, ja ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista, henkilöllisyyden todistamis- ja varmentamismenettelyjä ei tarvitse toistaa. Jos perustana olevaa sähköisen tunnistamisen menetelmää ei ole ilmoitettu, varmuustason ”korkea” on oltava asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen tai vastaavan elimen vahvistama ja on ryhdytty toimiin sen osoittamiseksi, että sen menettelyn tulokset, jossa ilmoitettu sähköisen tunnistamisen menetelmä aiemmin myönnettiin, ovat edelleen voimassa. TAI 2. Jos hakija ei esitä valokuvaa tai biometristä tunnistetta, sovelletaan samoja menettelyjä, joita tällaisen hyväksytyn valokuvan tai biometrisen todisteen saamiseksi käytetään kansallisella tasolla rekisteröinnistä vastaavan tahon jäsenvaltiossa.

([1]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008, annettu 9 päivänä heinäkuuta 2008, tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (EUVL L 218, 13.8.2008, s. 30).

2.1.3 Henkilöllisyyden todistaminen ja varmentaminen (oikeushenkilö)

Varmuustaso	Tarvittavat osatekijät
Matala	1. Oikeushenkilön ilmoitettu henkilöllisyys osoitetaan sen jäsenvaltion hyväksymällä todisteella, jossa sähköisen tunnistamisen menetelmää haetaan.

Varmuustaso	Tarvittavat osatekijät
	2. Todiste näyttää olevan voimassa ja sen voidaan olettaa olevan aito tai luotettavan lähteen mukaan olemassa oleva, jos oikeushenkilön kirjaaminen luotettavaan lähteeseen on vapaaehtoista ja sitä säännellään oikeushenkilön ja luotettavan lähteen välisellä järjestelyllä. 3. Luotettavan lähteen tiedossa ei ole, että oikeushenkilö olisi asemassa, joka estää sitä toimimasta kyseisenä oikeushenkilönä.
Korotettu	Sama kuin tasolla ”matala”, minkä lisäksi yhden kohdissa 1–3 mainituista vaihtoehdoista on täytyttävä: 1. Oikeushenkilön ilmoitettu henkilöllisyys osoitetaan sen jäsenvaltion hyväksymällä todisteella, jossa sähköisen tunnistamisen menetelmää haetaan ja jossa mainitaan oikeushenkilön nimi, oikeudellinen muoto ja (tapauksen mukaan) rekisterinumero. ja todiste tarkistetaan sen määrittämiseksi, onko se on aito tai luotettavan lähteen mukaan olemassa oleva, jos oikeushenkilön kirjaaminen luotettavaan lähteeseen on pakollinen ehto oikeushenkilön toiminnalle ja on ryhdytty toimiin sen riskin minimoimiseksi, että oikeushenkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todistus on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; tai 2. Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät menettelyt tarjoavat vastaavan varmuuden kuin 2.1.3. kohdassa esitetyt menettelyt varmuustasolla ”korotettu”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavantasoisen varmuuden on vahvistanut asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin; tai 3. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on ”korotettu” tai ”korkea”, henkilöllisyyden todistamis- ja varmentamismenettelyjä ei tarvitse toistaa. Jos perustana olevaa sähköisen tunnistamisen menetelmää ei ole ilmoitettu, varmuustason ”korotettu” tai ”korkea” on oltava asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen tai vastaavan elimen vahvistama.
Korkea	Sama kuin tasolla ”korotettu”, minkä lisäksi yhden kohdissa 1–3 mainituista vaihtoehdoista on täytyttävä: 1. Oikeushenkilön ilmoitettu henkilöllisyys osoitetaan sen jäsenvaltion hyväksymällä todisteella, jossa sähköisen tunnistamisen menetelmää haetaan ja jossa mainitaan oikeushenkilön nimi, oikeudellinen muoto ja vähintään yksi kansallisessa yhteydessä käytetty oikeushenkilön yksilöllinen tunniste ja todiste on tarkastettu sen varmistamiseksi, että se on luotettavan lähteen mukaan voimassa; tai

Varmuustaso	Tarvittavat osatekijät
	2. Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät menettelyt tarjoavat vastaavan varmuuden kuin 2.1.3 kohdassa esitetyt menettelyt varmuustasolla ”korkea”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavantasoisen varmuuden on vahvistanut asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin ja on ryhdytty toimiin sen osoittamiseksi, että kyseisen aiemman menettelyn tulokset ovat edelleen voimassa; tai 3. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on ”korkea”, henkilöllisyyden todistamis- ja varmentamismenettelyjä ei tarvitse toistaa. Jos perustana olevaa sähköisen tunnistamisen menetelmää ei ole ilmoitettu, varmuustason ”korkea” on oltava asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen tai vastaavan elimen vahvistama ja on ryhdytty toimiin sen osoittamiseksi, että sen menettelyn tulokset, jossa ilmoitettu sähköisen tunnistamisen menetelmä aiemmin myönnettiin, ovat edelleen voimassa.

2.1.4 Luonnollisten ja oikeushenkilöiden sähköisen tunnistamisen menetelmien välinen kytkös

Luonnollisen henkilön sähköisen tunnistamisen menetelmän ja oikeushenkilön sähköisen tunnistamisen menetelmän väliseen kytkökseen (jäljempänä tässä liitteessä ”kytkös”) sovelletaan soveltuvin osin seuraavia ehtoja:

1) Kytköksen voimassaolo on voitava keskeyttää ja/tai peruuttaa. Kytköksen elinkaarta (esim. aktivointi, voimassaolon keskeyttäminen, uusiminen tai peruuttaminen) hallinnoidaan kansallisesti hyväksyttyjen menettelyjen mukaisesti.

2) Luonnollinen henkilö, jonka sähköisen tunnistamisen menetelmä kytketään oikeushenkilön sähköisen tunnistamisen menetelmään, voi siirtää kytköksen toteuttamisen toiselle luonnolliselle henkilölle kansallisesti hyväksyttyjen menettelyjen mukaisesti. Vastuu säilyy kuitenkin siirtävällä luonnollisella henkilöllä.

3) Kytkös on tehtävä seuraavalla tavalla:

Varmuustaso	Tarvittavat osatekijät
Matala	1. Oikeushenkilön puolesta toimivan luonnollisen henkilön henkilöllisyyden todistamisen varmennetaan tapahtuneen vähintään tasolla ”matala”. 2. Kytkös on vahvistettu kansallisesti hyväksyttyjen menettelyjen mukaisesti. 3. Luotettavan lähteen tiedossa ei ole, että luonnollinen henkilö olisi asemassa, joka estää häntä toimimasta oikeushenkilön puolesta.
Korotettu	Tason ”matala” 3 kohta lisättynä seuraavalla: 1. Oikeushenkilön puolesta toimivan luonnollisen henkilön henkilöllisyyden todistamisen varmennetaan tapahtuneen tasolla ”korotettu” tai ”korkea”.

Varmuustaso	Tarvittavat osatekijät
	2. Kytkös on vahvistettu kansallisesti hyväksyttyjen menettelyjen mukaisesti, joiden tuloksena kytkös on kirjattu luotettavaan lähteeseen. 3. Kytkös on varmennettu luotettavasta lähteestä saatavan tiedon perusteella.
Korkea	Tason ”matala” 3 kohta ja tason ”korotettu” 2 kohta lisättynä seuraavalla: 1. Oikeushenkilön puolesta toimivan luonnollisen henkilön henkilöllisyyden todistamisen varmennetaan tapahtuneen tasolla ”korkea”. 2. Kytkös on varmennettu kansallisessa yhteydessä käytetyn oikeushenkilöä edustavan yksilöllisen tunnisteen perusteella ja luotettavasta lähteestä saatavan, luonnollista henkilöä yksilöivästi edustavan tiedon perusteella.

2.2 *Sähköisen tunnistamisen menetelmien hallinta*

2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu

Varmuustaso	Tarvittavat osatekijät
Matala	1. Sähköisen tunnistamisen menetelmässä käytetään vähintään yhtä todentamistekijää. 2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että myöntäjä toteuttaa kohtuulliset toimenpiteet tarkistaakseen, että sitä käytetään vain sen henkilön hallinnassa tai hallussa, jolle se kuuluu.
Korotettu	1. Sähköisen tunnistamisen menetelmässä käytetään vähintään kahta todentamistekijää eri luokista. 2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.
Korkea	Taso ”korotettu” lisättynä seuraavalla: 1. Sähköisen tunnistamisen menetelmä on suojattu toisintamiselta ja väärentämiseltä sekä hyökkäyksiltä, joiden vakavuusaste on korkea (”high”). 2. Sähköisen tunnistamisen menetelmä on suunniteltu niin, että henkilö, jolle se kuuluu, voi suojata sen luotettavasti muiden käytöltä.

2.2.2 Myöntäminen, toimittaminen ja aktivointi

Varmuustaso	Tarvittavat osatekijät
Matala	Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta sen voidaan olettaa saavuttavan vain aiotun henkilön.
Korotettu	Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta se voidaan olettaa toimitettavan vain sen henkilön haltuun, jolle se kuuluu.
Korkea	Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu.

2.2.3 Voimassaolon keskeyttäminen, peruuttaminen ja uudelleenaktivointi

Varmuustaso	Tarvittavat osatekijät
Matala	1. Sähköisen tunnistamisen menetelmän voimassaolo on mahdollista keskeyttää ja/tai peruuttaa viivyttelemättä ja tehokkaasti. 2. Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi. 3. Uudelleenaktivoinnin ehtona on, että ennen voimassaolon keskeyttämistä tai peruuttamista asetetut varmuusvaatimukset täyttyvät edelleen.
Korotettu	Sama kuin tasolla ”matala”.
Korkea	Sama kuin tasolla ”matala”.

2.2.4 Uusiminen ja korvaaminen

Varmuustaso	Tarvittavat osatekijät
Matala	Ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista uusimisen tai korvaamisen on täytettävä samat varmuusvaatimukset kuin henkilöllisyyden alkuperäisen todistamisen ja varmentamisen yhteydessä tai sen on perustuttava saman tai korkeamman varmuustason voimassa olevaan sähköisen tunnistamisen menetelmään.
Korotettu	Sama kuin tasolla ”matala”.
Korkea	Taso ”matala” lisättynä seuraavalla: Jos uusiminen tai korvaaminen perustuu voimassa olevaan sähköisen tunnistamisen menetelmään, tunnistetiedot varmennetaan luotettavasta lähteestä.

2.3 *Todentaminen*

Tässä jaksossa käsitellään todentamismekanismin käyttöön liittyviä uhkia ja luetellaan vaatimukset kullekin varmuustasolle. Tässä jaksossa turvatoimenpiteet on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.

2.3.1 Todentamismekanismi

Seuraavassa taulukossa esitetään vaatimukset varmuustasoittain todentamismekanismista, jolla luonnollinen tai oikeushenkilö käyttää sähköisen tunnistamisen menetelmää vahvistaakseen henkilöllisyytensä luottavalle osapuolelle.

Varmuustaso	Tarvittavat osatekijät
Matala	1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen. 2. Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella. 3. Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkeampaa perustasoa (”enhanced-basic”), voi heikentää todentamismekanismeja.

Varmuustaso	Tarvittavat osatekijät
Korotettu	Taso ”matala” lisättynä seuraavalla: 1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käyttämällä dynaamista todentamista. 2. Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen (”moderate”), voi heikentää todentamismekanismeja.
Korkea	Taso ”korotettu” lisättynä seuraavalla: Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkea (”high”), voi heikentää todentamismekanismeja.

2.4 *Hallinto ja organisointi*

Kaikilla osallistujilla, jotka tarjoavat sähköiseen tunnistamiseen liittyvää rajat ylittävää palvelua (jäljempänä tässä liitteessä ”palveluntarjoajat”), on oltava käytössä dokumentoidut tietoturvallisuuden hallintakäytännöt, toimintaperiaatteet, lähestymistavat riskien hallintaan ja muut hyväksytyt turvatoimenpiteet siten, että asiaankuuluvilla sähköisen tunnistamisen järjestelmien hallintoelimillä on kyseeseen tulevissa jäsenvaltioissa varmuus siitä, että tehokkaat menettelyt ovat käytössä. Kaikki 2.4 jakson vaatimukset/osatekijät on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.

2.4.1 Yleiset säännökset

Varmuustaso	Tarvittavat osatekijät
Matala	1. Palveluntarjoajat, jotka tarjoavat tämän asetuksen soveltamisalaan kuuluvaa operatiivista palvelua, ovat viranomaisia tai jäsenvaltion lainsäädännössä tunnustettuja oikeushenkilöitä, joilla on vakiintunut organisaatio ja jotka ovat täysin toiminnallisia kaikilla palvelujen tarjoamisen kannalta merkityksellisillä toimintalohkoilla. 2. Tarjoajat täyttävät kaikki oikeudelliset vaatimukset, jotka koskevat niitä liittyen palvelun harjoittamiseen ja tarjoamiseen, mukaan lukien niiden tietojen luokat, joita voidaan pyytää, henkilöllisyyden todistamistavat sekä tiedot, joita voidaan säilyttää, ja ajanjaksot, joiden ajan niitä voidaan säilyttää. 3. Palveluntarjoajat voivat osoittaa valmiutensa ottaa vahinkovastuuriski, ja niillä on riittävät taloudelliset varat turvata toiminnan jatkuminen ja palvelujen tarjoaminen. 4. Palveluntarjoajat ovat vastuussa mahdollisten muille tahoille ulkoistettujen sitoumusten täyttämisestä ja järjestelmän toimintaperiaatteiden noudattamisesta samalla tavoin kuin jos palveluntarjoajat olisivat suorittaneet tehtävät itse. 5. Sähköisen tunnistamisen järjestelmille, jotka eivät perustu kansalliseen lakiin, on oltava tehokas suunnitelma järjestelmän päättämisen varalta. Tällaisen suunnitelman on sisällettävä palvelun hallittu lopettaminen tai siirto toiselle palveluntarjoajalle, tapa ilmoittaa tästä asiaankuuluville viranomaisille ja loppukäyttäjille sekä tiedot siitä, miten järjestelmään kirjatut tiedot suojataan, säilytetään ja hävitetään järjestelmän toimintaperiaatteiden mukaisesti.
Korotettu	Sama kuin tasolla ”matala”.
Korkea	Sama kuin tasolla ”matala”.

2.4.2 Julkaistut ilmoitukset ja käyttäjätiedot

Varmuustaso	Tarvittavat osatekijät
Matala	1. Käytössä on julkaistu palvelun määritelmä, joka sisältää kaikki sovellettavat ehdot, edellytykset ja maksut, mukaan lukien mahdolliset käyttörajoitukset. Palvelun määritelmään on sisällytettävä tietosuojaperiaatteet. 2. Käyttöön on otettava asianmukaiset toimintaperiaatteet ja menettelyt sen varmistamiseksi, että palvelun käyttäjille ilmoitetaan hyvissä ajoin ja luotettavasti kaikista muutoksista palvelun määritelmässä ja sovellettavissa ehdoissa, edellytyksissä ja tietosuojaperiaatteissa kulloisenkin palvelun osalta. 3. Käyttöön on otettava asianmukaiset toimintaperiaatteet ja menettelyt, jotta voidaan antaa asianmukaiset ja täydelliset vastaukset tietopyyntöihin.
Korotettu	Sama kuin tasolla ”matala”.
Korkea	Sama kuin tasolla ”matala”.

2.4.3 Tietoturvallisuuden hallinta

Varmuustaso	Tarvittavat osatekijät
Matala	Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.
Korotettu	Taso ”matala” lisättynä seuraavalla: Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.
Korkea	Sama kuin tasolla ”korotettu”.

2.4.4 Tietojen säilyttäminen

Varmuustaso	Tarvittavat osatekijät
Matala	1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojaan ja tietojen säilyttämiseen liittyvät hyvät käytännöt. 2. Järjestelmään kirjatut tiedot säilytetään siltä osin kuin tämä on kansallisen lainsäädännön tai muun kansallisen hallinnollisen järjestelyn mukaan sallittua ja suojataan niin kauan kuin niitä tarvitaan tarkastuksia ja tietoturvaloukkausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti.
Korotettu	Sama kuin tasolla ”matala”.
Korkea	Sama kuin tasolla ”matala”.

2.4.5 Tilat ja henkilökunta

Seuraavassa taulukossa esitetään vaatimukset, jotka koskevat tiloja ja henkilöstöä sekä tarvittaessa alihankkijoita, jotka suorittavat tämän asetuksen soveltamisalaan kuuluvia tehtäviä. Kunkin vaatimuksen noudattaminen on suhteutettava siihen, minkä tasoinen riski tarjottavaan varmuustasoon liittyy.

Varmuustaso	Tarvittavat osatekijät
Matala	1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä. 2. Käytössä on riittävästi henkilöstöä ja alihankkijoita, jotta palvelua voidaan toteuttaa ja resursoida asianmukaisesti sen toimintaperiaatteiden ja menettelyjen mukaisesti. 3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen. 4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että pääsy alueille, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita.
Korotettu	Sama kuin tasolla ”matala”.
Korkea	Sama kuin tasolla ”matala”.

2.4.6 Tekniset tarkastukset

Varmuustaso	Tarvittavat osatekijät
Matala	1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi. 2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta. 3. Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja sovelluksiin, jotka edellyttävät tällaista pääsyä. On varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä. 4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin. 5. Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.
Korotettu	Sama kuin tasolla ”matala” lisättynä seuraavalla: Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.
Korkea	Sama kuin tasolla ”korotettu”.

2.4.7 Noudattaminen ja tarkastus

Varmuustaso	Tarvittavat osatekijät
Matala	Määräajoin tehdään sisäisiä tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

Varmuustaso	Tarvittavat osatekijät
Korotettu	Määräajoin tehdään riippumattomia sisäisiä tai ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.
Korkea	1. Määräajoin tehdään riippumattomia ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen. 2. Jos järjestelmää hallinnoi suoraan julkinen elin, tarkastukset tehdään kansallisen lainsäädännön mukaisesti.