KOMISJONI RAKENDUSMÄÄRUS (EL) 2015/1502,

8. september 2015,

millega kehtestatakse e-identimise vahendite usaldusväärsuse tasemete minimaalsed tehnilised kirjeldused ja menetlused vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 8 lõikele 3

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ), [1] eriti selle artikli 8 lõiget 3,

ning arvestades järgmist:

(1) Määruse (EL) nr 910/2014 artiklis 8 on sätestatud, et e-identimise süsteemis, millest on teavitatud artikli 9 lõike 1 kohaselt, määratakse süsteemi raames väljastatud e-identimise vahendite madal, märkimisväärne ja/või kõrge usaldusväärsuse tase.

(2) Minimaalsete tehniliste kirjelduste, standardite ja menetluste kindlaksmääramine on hädavajalik, et tagada usaldusväärsuse tasemete üksikasjade ühene mõistmine ja kindlustada koostalitlusvõime teatatud e-identimise süsteemide riigisiseste usaldusväärsuse tasemete vastavusse viimisel artikli 8 kohaste usaldusväärsuse tasemetega, nagu on sätestatud määruse (EL) nr 910/2014 artikli 12 lõike 4 punktis b.

(3) Käesolevas rakendusaktis sätestatud kirjeldustes ja menetlustes on lähtutud rahvusvahelisest standardist ISO/IEC 29115, mis on peamine rahvusvaheline standard e-identimise vahendite usaldusväärsuse tasemete valdkonnas. Määruse (EL) nr 910/2014 sisu erineb siiski nimetatud rahvusvahelisest standardist eeskätt identiteedi tõestamise ja kontrollimise nõuete osas, aga ka selles osas, kuidas võetakse arvesse erinevusi liikmesriikide identiteedi-süsteemide ja ELis samal otstarbel kasutatavate vahendite vahel. Kuigi käesoleva dokumendi lisa toetub nimetatud rahvusvahelisele standardile, ei tuleks seal seetõttu konkreetselt viidata standardi ISO/IEC 29115 sisule.

(4) Käesoleva määruse koostamisel kasutati kõige otstarbekamaks peetud tulemuspõhist lähenemisviisi ning seda on näha ka terminite ja mõistete määratlustest. Neis võetakse arvesse määruse (EL) nr 910/2014 eesmärki e-identimise vahendite usaldusväärsuse tasemete puhul. Seepärast tuleks käesolevas rakendusaktis sätestatud kirjelduste ja menetluste juurutamisel võtta täiel määral arvesse nii suurprojekti STORK ja selle raames välja töötatud kirjeldusi kui ka standardi ISO/IEC 29115 määratlusi ja mõisteid.

(5) Olenevalt sellest, millises kontekstis tuleb identiteedi tõestamise mõnd aspekti kontrollida, võivad autoriteetsed allikad olla erinevad (nt registrid, dokumendid, organid jms). Eri liikmesriikides võivad autoriteetsed allikad olla erinevad isegi siis, kui kontekst on sarnane.

(6) Identiteedi tõestamise ja kontrollimise nõuetes tuleks arvestada erinevate süsteemide ja tavadega ning tagada samas vajaliku usalduse loomiseks piisavalt kõrge usaldusväärsuse tase. Seetõttu peaks varem muul otstarbel kui e-identimise vahendite väljastamiseks kasutatud menetluste heakskiitmise eeltingimuseks olema kinnitus, et nende menetluste puhul on täidetud vastava usaldusväärsuse taseme jaoks ette nähtud nõuded.

[1] ELT L 257, 28.8.2014, lk 73.

(7) Tavaliselt kasutatakse teatavaid autentimistegureid, milleks võib olla ühissaladus, füüsiline seade või füüsiline atribuut. Autentimisprotsessi turvalisuse suurendamiseks tuleks siiski soodustada rohkemate, eelistatavalt eri kategooriatesse kuuluvate autentimistegurite kasutamist.

(8) Käesolev määrus ei tohiks mõjutada juriidiliste isikute esindamise õigust. Lisas tuleks siiski ette näha nõuded füüsiliste ja juriidiliste isikute e-identimise vahendite sidumiseks.

(9) Tuleks tunnustada infoturbe ja teenuste juhtimise süsteemide olulisust ning tunnustatud metoodikate kasutamise ja standardites (nt ISO/IEC 27000 ja standardisari ISO/IEC 20000) esitatud põhimõtete rakendamise olulisust.

(10) Samuti tuleks arvesse võtta liikmesriikide häid tavasid usaldusväärsuse tasemete vallas.

(11) Rahvusvahelistel standarditel põhinev IT-turbe sertifitseerimine on oluline vahend, et kontrollida toote turvalisuse vastavust käesolevas rakendusaktis sätestatud nõuetele.

(12) Määruse (EL) nr 910/2014 artiklis 48 osutatud komitee ei esitanud arvamust oma esimehe kehtestatud tähtaja jooksul,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

1. Teatatud e-identimise süsteemi alusel väljastatud e-identimise vahendite madal, märkimisväärne või kõrge usaldusväärsuse tase määratakse kindlaks lisas sätestatud kirjelduste ja menetluste põhjal.

2. Lisas esitatud kirjeldusi ja menetlusi kasutatakse teatatud e-identimise süsteemi alusel väljastatud e-identimise vahendite usaldusväärsuse taseme täpsustamiseks, määrates selleks kindlaks järgmiste komponentide usaldatavuse ja kvaliteedi:

a) väljastamine käesoleva määruse lisa punktis 2.1 sätestatud tähenduses vastavalt määruse (EL) nr 910/2014 artikli 8 lõike 3 punktile a;

b) e-identimise vahendite haldamine käesoleva määruse lisa punktis 2.2 sätestatud tähenduses vastavalt määruse (EL) nr 910/2014 artikli 8 lõike 3 punktidele b ja f;

c) autentimine käesoleva määruse lisa punktis 2.3 sätestatud tähenduses vastavalt määruse (EL) nr 910/2014 artikli 8 lõike 3 punktile c;

d) haldamine ja korraldamine käesoleva määruse lisa punktis 2.4 sätestatud tähenduses vastavalt määruse (EL) nr 910/2014 artikli 8 lõike 3 punktidele d ja e.

3. Kui teatatud e-identimise süsteemi alusel väljastatud e-identimise vahendid vastavad usaldusväärsuse kõrgema taseme nõudele, eeldatakse, et nad vastavad samale nõudele ka usaldusväärsuse madalama taseme puhul.

4. Kui lisa asjaomases osas ei ole sätestatud teisiti, peavad konkreetse usaldusväärsuse taseme saavutamiseks olema nõuded täidetud kõigi komponentide puhul, mis on lisas loetletud seoses e-identimise süsteemi alusel väljastatud e-identimise vahendi selle usaldusväärsuse tasemega.

Artikkel 2

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 8. september 2015

Komisjoni nimel
president
Jean-Claude JUNCKER

LISA

Teatatud e-identimise süsteemi alusel väljastatud e-identimise vahendite usaldusväärsuse madala, märkimisväärse ja kõrge taseme minimaalsed tehnilised kirjeldused ja menetlused

1. **Kasutatud mõisted**

Käesolevas lisas kasutatakse järgmisi mõisteid:

1) „autoriteetne allikas" – mis tahes allikas, ükskõik millises vormis, mille puhul võib kindel olla, et sealt saadavad andmed, teave ja/või tõendid on täpsed ja neid saab kasutada identiteedi tõendamiseks;

2) „autentimistegur" – tegur, mille puhul on kinnitatud tema seotus konkreetse isikuga ja mis kuulub ühte järgmistest kategooriatest:

   a) „millegi omamisel põhinev autentimistegur" – autentimistegur, mille puhul peab subjekt tõendama, et tal on see olemas;

   b) „teabel põhinev autentimistegur" – autentimistegur, mille puhul peab subjekt tõendama, et ta teab seda;

   c) „olemuslik autentimistegur" – autentimistegur, mis põhineb füüsilise isiku füüsilisel omadusel ja mille puhul peab subjekt tõendama, et tal on see füüsiline omadus;

3) „dünaamiline autentimine" – elektrooniline protsess, mille käigus kasutatakse krüpteerimist või muid meetodeid, mis võimaldavad nõudluspõhiselt luua elektroonilise tõendi, et subjekt valdab või omab identimisandmeid, ning mis muutub iga kord, kui subjekt autenditakse subjekti identiteeti kontrollivas süsteemis;

4) „infoturbe haldamise süsteem" – protsesside ja menetluste kogum, mille eesmärk on viia infoturbega seotud riskid vastuvõetavale tasemele.

2. **Tehnilised kirjeldused ja menetlused**

Käesolevas lisas kirjeldatud tehniliste kirjelduste ja menetluste komponente kasutatakse selleks, et teha kindlaks, kuidas kohaldatakse e-identimise süsteemi alusel väljastatud e-identimise vahendite suhtes määruse (EL) nr 910/2014 artikli 8 nõudeid ja kriteeriume.

2.1. *Väljastamine*

2.1.1. Taotluse esitamine ja registreerimine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Veendutakse, et taotluse esitaja on teadlik e-identimise vahendi kasutamise tingimustest. 2. Veendutakse, et taotluse esitaja on teadlik e-identimise vahendi kasutamisega seotud soovituslikest ettevaatusabinõudest. 3. Kogutakse identiteedi tõestamiseks ja kontrollimiseks vajalikud identiteediandmed.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.1.2. Identiteedi tõestamine ja kontrollimine (füüsilise isiku puhul)

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Võib eeldada, et isikul on väidetava identiteedi kohta tõendid, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse. 2. Võib eeldada, et tõendid on ehtsad või autoriteetse allika andmetel olemas ning tõendid tunduvad olevat kehtivad. 3. Autoriteetsele allikale tuginedes on teada, et väidetav identiteet on olemas, ning võib eeldada, et see identiteet on ka tegelikult isikul, kes väidab selle endal olevat.
Märkimisväärne	Lisaks madala taseme nõuetele peab olema täidetud üks punktides 1–4 loetletud tingimus: 1. on kontrollitud, et isikul on oma väidetava identiteedi kohta tõendid, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse, ja tal on väidetav identiteet ka tegelikult, ning tõendeid on kontrollitud, et veenduda nende ehtsuses, või on tõendid autoriteetse allika andmetel olemas ja seotud reaalse isikuga ning võetud on meetmed minimeerimaks riski, et isiku väidetav identiteet ei ole tema tegelik identiteet; sealjuures võetakse arvesse näiteks tõendi kadumise, varastamise, selle kehtivuse peatamise, tühistamise või aegumise riski, või 2. liikmesriigis, kus dokument on väljastatud, esitatakse registreerimisprotsessi käigus identiteeti tõendav dokument, mis osutub olevat seotud isikuga, kes selle esitab, ning võetud on meetmed minimeerimaks riski, et isiku väidetav identiteet ei ole tema tegelik identiteet; sealjuures võetakse arvesse näiteks dokumentide kadumise, varastamise, nende kehtivuse peatamise, tühistamise või aegumise riski, või 3. kui menetlus, mida avalik-õiguslik või eraõiguslik isik on samas liikmesriigis varem kasutanud muul otstarbel kui e-identimise vahendite väljastamiseks, tagab samaväärse usaldusväärsuse taseme kui punktis 2.1.2 sätestatud märkimisväärne usaldusväärsuse tase, ei pea registreerimise eest vastutav isik varasemaid menetlusi kordama, kui usaldusväärsuse samaväärsust kinnitab Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 765/2008 ([1]) artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne asutus, või 4. kui e-identimise vahend väljastatakse märkimisväärse või kõrge usaldusväärsuse tasemega kehtiva teatatud e-identimise vahendi põhjal ning võttes arvesse isiku identimisandmete muutumise riske, ei ole identiteedi tõestamise ja kontrollimise protsessi vaja korrata. Kui aluseks võetavast e-identimise vahendist ei ole teavitatud, peab märkimisväärset või kõrget usaldusväärsuse taset kinnitama määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne organ.

Usaldusväärsuse tase	Vajalikud komponendid
Kõrge	Täidetud peavad olema kas punkti 1 või 2 nõuded. 1. Lisaks märkimisväärse taseme nõuetele peab olema täidetud üks punktides a–c loetletud tingimus: a) kui on kontrollitud, et isikul on fotoga või biomeetriline identimist võimaldav tõend, mida tunnustab liikmesriik, kus esitatakse taotlus e-identimise vahendi saamiseks, ja see tõend vastab väidetavale identiteedile, veendutakse, et tõend on autoriteetse allika andmetel kehtiv, ning taotluse esitaja samasus väidetava identiteediga tuvastatakse, võrreldes isiku üht või mitut füüsilist omadust autoriteetse allikaga, või b) kui menetlus, mida avalik-õiguslik või eraõiguslik isik on samas liikmesriigis varem kasutanud muul otstarbel kui e-identimise vahendite väljastamiseks, tagab samaväärse usaldusväärsuse taseme kui punktis 2.1.2 sätestatud kõrge usaldusväärsuse tase, ei pea registreerimise eest vastutav isik varasemaid menetlusi kordama, kui usaldusväärsuse samaväärsust kinnitab määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne asutus, ning võetakse meetmeid tõendamaks, et varasema menetluse tulemused kehtivad endiselt, või c) kui e-identimise vahend väljastatakse kõrge usaldusväärsuse tasemega kehtiva teatatud e-identimise vahendi põhjal ning võttes arvesse isiku identimisandmete muutumise riske, ei ole identiteedi tõestamise ja kontrollimise protsessi vaja korrata. Kui aluseks võetavast e-identimise vahendist ei ole teavitatud, peab kõrget usaldusväärsuse taset kinnitama määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne organ, ning võetakse meetmeid tõendamaks, et teatatud e-identimise vahendi väljastamise varasema menetluse tulemused kehtivad endiselt, või 2. kui taotluse esitaja ei esita fotoga või biomeetrilist identimist võimaldavat tunnustatud tõendit, kohaldatakse samasugust menetlust nagu kasutatakse sellise tunnustatud fotoga või biomeetrilist identimist võimaldava tõendi saamiseks riigisisesel tasemel registreerimise eest vastutava isiku liikmesriigis.

([1]) Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 765/2008, 9. juuli 2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30).

2.1.3. Identiteedi tõestamine ja kontrollimine (juriidiliste isikute puhul)

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Juriidilise isiku väidetavat identiteeti tõendatakse tõendi alusel, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse.

Usaldusväärsuse tase	Vajalikud komponendid
	2. Tõend tundub olevat kehtiv ning võib eeldada, et see on ehtne või autoriteetse allika andmetel olemas, kui juriidilise isiku lisamine autoriteetsesse allikasse on vabatahtlik ja seda reguleerib juriidilise isiku ja autoriteetse allika vaheline kokkulepe. 3. Autoriteetse allika andmetel ei ole juriidilise isiku seisund selline, mis takistaks teda kõnealuse juriidilise isikuna tegutsemast.
Märkimisväärne	Lisaks madala taseme nõuetele peab olema täidetud üks punktides 1–3 loetletud tingimus. 1. Juriidilise isiku väidetavat identiteeti tõendatakse tõendite alusel, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse, ja milles on kirjas juriidilise isiku nimi, õiguslik vorm ja (vajaduse korral) registreerimisnumber, ning tõendit kontrollitakse, et veenduda, kas see on ehtne või autoriteetse allika andmetel olemas, kui juriidilise isiku lisamine autoriteetsesse allikasse on nõutav, et juriidiline isik saaks oma valdkonnas tegutseda, ning võetud on meetmed minimeerimaks riski, et väidetav identiteet ei ole juriidilise isiku tegelik identiteet; sealjuures võetakse arvesse näiteks dokumentide kadumise, varastamise, nende kehtivuse peatamise, tühistamise või aegumise riski, või 2. kui menetlus, mida avalik-õiguslik või eraõiguslik isik on samas liikmesriigis varem kasutanud muul otstarbel kui e-identimise vahendite väljastamiseks, tagab samaväärse usaldusväärsuse taseme kui punktis 2.1.3 sätestatud märkimisväärne usaldusväärsuse tase, ei pea registreerimise eest vastutav isik varasemaid menetlusi kordama, kui usaldusväärsuse samaväärsust kinnitab määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne asutus, või 3. kui e-identimise vahend väljastatakse märkimisväärse või kõrge usaldusväärsuse tasemega kehtiva teatatud e-identimise vahendi põhjal, ei ole identiteedi tõestamise ja kontrollimise protsessi vaja korrata. Kui aluseks võetavast e-identimise vahendist ei ole teavitatud, peab märkimisväärset või kõrget usaldusväärsuse taset kinnitama määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne organ.
Kõrge	Lisaks märkimisväärse taseme nõuetele peab olema täidetud üks punktides 1–3 loetletud tingimus. 1. Juriidilise isiku väidetavat identiteeti tõendatakse tõendite alusel, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse, ja milles on kirjas juriidilise isiku nimi, õiguslik vorm ja vähemalt üks kordumatu tunnus, mida kasutatakse riigi sees juriidilise isiku tähistamiseks, ning tõendeid on kontrollitud veendumaks, et need on autoriteetse allika andmetel kehtivad, või

Usaldusväärsuse tase	Vajalikud komponendid
	2. kui menetlus, mida avalik-õiguslik või eraõiguslik isik on samas liikmesriigis varem kasutanud muul otstarbel kui e-identimise vahendite väljastamiseks, tagab samaväärse usaldusväärsuse taseme kui punktis 2.1.3 sätestatud kõrge usaldusväärsuse tase, ei pea registreerimise eest vastutav isik varasemaid menetlusi kordama, kui usaldusväärsuse samaväärsust kinnitab määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne asutus, ning võetakse meetmeid tõendamaks, et nimetatud eelmise menetluse tulemused kehtivad endiselt, või 3. kui e-identimise vahend väljastatakse kõrge usaldusväärsuse tasemega kehtiva teatatud e-identimise vahendi põhjal, ei ole identiteedi tõestamise ja kontrollimise protsessi vaja korrata. Kui aluseks võetavast e-identimise vahendist ei ole teavitatud, peab kõrget usaldusväärsuse taset kinnitama määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne organ, ning võetakse meetmeid tõendamaks, et teatatud e-identimise vahendi väljastamise varasema menetluse tulemused kehtivad endiselt.

2.1.4. Füüsiliste ja juriidiliste isikute e-identimise vahendite seostamine

Vajaduse korral kehtivad füüsilise isiku e-identimise vahendi ja juriidilise isiku e-identimise vahendi omavahelise seostamise (edaspidi „seostamine") suhtes järgmised tingimused.

1) Seostamist peab olema võimalik peatada ja/või kehtetuks tunnistada. Seostamistsüklit (st aktiveerimist, peatamist, uuendamist, kehtetuks tunnistamist) hallatakse riiklikult tunnustatud menetluste kohaselt.

2) Füüsiline isik, kelle e-identimise vahend on seostatud juriidilise isiku e-identimise vahendiga, võib delegeerida seostamisest tulenevad toimingud riiklikult tunnustatud menetluse kohaselt teisele füüsilisele isikule. Vastutavaks jääb siiski füüsiline isik, kes toimingud delegeeris.

3) Seostamine toimub järgmiselt.

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Kontrollitakse, et juriidilise isiku nimel tegutseva füüsilise isiku identiteet on tõestatud vähemalt madala usaldusväärsuse taseme nõuete kohaselt. 2. Seostamine on toimunud riiklikult tunnustatud menetluse kohaselt. 3. Autoriteetse allika andmetel ei ole füüsilise isiku seisund selline, mis takistaks teda juriidilise isiku nimel tegutsemast.
Märkimisväärne	Lisaks madala taseme punktile 3 peavad olema täidetud järgmised tingimused. 1. Kontrollitakse, et juriidilise isiku nimel tegutseva füüsilise isiku identiteedi tõestamine on toimunud märkimisväärse või kõrge usaldusväärsuse tasemega.

Usaldusväärsuse tase	Vajalikud komponendid
	2. Seostamine on toimunud riiklikult tunnustatud menetluse kohaselt, mille tulemusena registreeriti seostamine autoriteetses allikas. 3. Seostatust on kontrollitud autoriteetse allika teabe põhjal.
Kõrge	Lisaks madala taseme punktile 3 ja märkimisväärse taseme punktile 2 peavad olema täidetud järgmised tingimused. 1. Kontrollitakse, et juriidilise isiku nimel tegutseva füüsilise isiku identiteedi tõestamine on toimunud kõrge usaldusväärsuse tasemega. 2. Seostatust on kontrollitud kordumatu tunnuse põhjal, mida kasutatakse riigi sees juriidilise isiku tähistamiseks, ja füüsilist isikut tähistava autoriteetsest allikast pärit kordumatu teabe põhjal.

2.2. *E-identimise vahendite haldamine*

2.2.1. E-identimise vahendite tunnused ja disain

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. E-identimise vahend kasutab vähemalt üht autentimistegurit. 2. E-identimise vahend on kavandatud selliselt, et selle väljastaja võtab mõistlikke meetmeid veendumaks, et vahendit kasutatakse ainult selle isiku kontrolli all või selle isiku poolt, kelle oma see on.
Märkimisväärne	1. E-identimise vahend kasutab vähemalt kaht eri kategooriate autentimistegurit. 2. E-identimise vahend on kavandatud selliselt, et võib eeldada, et seda kasutatakse vaid selle isiku kontrolli all või selle isiku poolt, kelle oma see on.
Kõrge	Lisaks märkimisväärsele tasemele peavad olema täidetud järgmised tingimused. 1. E-identimise vahend on kaitstud kopeerimise ja manipuleerimise ning suure ründepotentsiaaliga ründajate vastu. 2. E-identimise vahend on kavandatud selliselt, et selle omanik saab seda kindlalt kaitsta teiste isikute poolse kasutamise eest.

2.2.2. Väljastamine, üleandmine ja aktiveerimine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	Pärast väljastamist antakse e-identimise vahend üle sellise mehhanismi kaudu, mille puhul võib eeldada, et vahend jõuab vaid selle isikuni, kellele see on mõeldud.
Märkimisväärne	Pärast väljastamist antakse e-identimise vahend üle sellise mehhanismi kaudu, mille puhul võib eeldada, et vahend antakse üle vaid selle isiku kätte, kellele see kuulub.
Kõrge	Aktiveerimisprotsessi käigus kontrollitakse, et e-identimise vahend anti üle vaid selle isiku kätte, kellele ta kuulub.

2.2.3. Kehtivuse peatamine, kehtetuks tunnistamine ja taasaktiveerimine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. E-identimise vahendi kehtivust on võimalik kiiresti ja tõhusalt peatada ja/või see kehtetuks tunnistada. 2. Olemas on meetmed, mille abil takistatakse ilma loata kehtivuse peatamist, kehtetuks tunnistamist ja/või uuesti aktiveerimist. 3. Uuesti aktiveerimine toimub ainult siis, kui endiselt on täidetud samad usaldusväärsuse nõuded kui enne kehtivuse peatamist või kehtetuks tunnistamist.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.2.4. Uuendamine ja asendamine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	Võttes arvesse isiku identiteediandmete muutumise riske, peavad uuendamine ja asendamine vastama samadele usaldusväärsuse nõuetele kui esialgne identiteedi tõestamine ja kontrollimine või põhinema sama või kõrgema usaldusväärsuse tasemega kehtival e-identimise vahendil.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Lisaks madalale tasemele peavad olema täidetud järgmised tingimused. Kui uuendamine või asendamine põhineb kehtival e-identimise vahendil, kontrollitakse identiteediandmeid autoriteetsest allikast.

2.3. *Autentimine*

Selles punktis keskendutakse autentimismehhanismi kasutamisega seotud ohtudele ning loetletakse iga usaldusväärsuse taseme nõuded. Käesoleva punkti tähenduses loetakse turvameetmed konkreetse taseme riskidega vastavuses olevaiks.

2.3.1. Autentimismehhanism

Järgmises tabelis on esitatud nõuded igale sellise autentimismehhanismi usaldusväärsuse tasemele, mille kaudu füüsiline või juriidiline isik kasutab e-identimise vahendit selleks, et kinnitada oma isikusamasust tuginevale isikule.

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Enne isiku identiteediandmete loovutamist tuleb usaldusväärselt kontrollida e-identimise vahendit ja selle kehtivust. 2. Kui isiku identiteediandmed on salvestatud autentimismehhanismi osana, peab see teave olema turvatud, et kaitsta seda kadumise või rikkumise, sh väljaspool võrku analüüsimise eest. 3. Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et baasoskustest suurema ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.

Usaldusväärsuse tase	Vajalikud komponendid
Märkimisväärne	Lisaks madalale tasemele peavad olema täidetud järgmised tingimused. 1. Enne isiku identiteediandmete loovutamist tuleb e-identimise vahendit ja selle kehtivust usaldusväärselt kontrollida dünaamilise autentimisega. 2. Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et keskmise ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.
Kõrge	Lisaks märkimisväärsele tasemele peavad olema täidetud järgmised tingimused. Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et suure ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.

2.4. *Haldamine ja korraldamine*

Kõik osalised, kes osutavad piiriüleselt e-identimisega seotud teenust (edaspidi „teenuseosutajad"), peavad kasutama dokumenteeritud infoturbe haldamise tavasid, põhimõtteid, lähenemisviise riskihaldusele ja muid tunnustatud turvameetmeid, et asjaomaste liikmesriikide e-identimise süsteemide juhtimisega tegelevad asutused saaksid olla kindlad, et kasutatakse tõhusaid tegutsemisviise. Punktis 2.4 loetakse kõik nõuded/komponendid konkreetse taseme riskidega vastavuses olevaiks.

2.4.1. Üldsätted

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Käesoleva määrusega hõlmatud põhiteenuse osutajaks on liikmesriigi õigusega tunnustatud riigiasutus või juriidiline üksus, millel on kindlakskujunenud struktuur ja mis on täiesti tegev kõigis teenuse osutamise seisukohast asjakohastes aspektides. 2. Teenuseosutajad täidavad kõiki õigusaktidest tulenevaid nõudeid, mis nende suhtes kehtivad seoses teenuse käitamise ja osutamisega, kaasa arvatud teabe liigid, mille kohta võib päringuid esitada, kuidas toimub identiteedi tõestamine ning millist teavet ja kui kaua tuleb säilitada. 3. Teenuseosutajad peavad tõendama oma suutlikkust tulla toime kahjude eest vastutamise riskiga ning piisavate rahaliste vahendite olemasolu tegevuse jätkamiseks ja teenuste osutamiseks. 4. Teenuseosutajad vastutavad kõigi teistelt üksustelt tellitud kohustuste täitmise eest ja süsteemi põhimõtete järgmise eest, nagu oleksid nad ise neid ülesandeid täitnud. 5. E-identimise süsteemide puhul, mis ei ole loodud riigi seadusega, peab olemas olema tõhus tegevuse lõpetamise kava. Sellises kavas tuleb käsitleda teenuse osutamise korrakohast lõpetamist või teenuse osutamise üleminekut teisele teenuseosutajale, asjaomaste asutuste ja lõppkasutajate teavitamist ning seda, kuidas andmikke süsteemi põhimõtete kohaselt kaitstakse, säilitatakse ja hävitatakse.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.4.2. Avaldatud teatised ja kasutajatele mõeldud teave

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Avaldatud kujul on olemas teenuse määratlus, mis hõlmab kõiki tingimusi ja tasusid, kaasa arvatud teenuse kasutamise võimalikke piiranguid. Teenuse määratlus peab sisaldama privaatsuspõhimõtteid. 2. Kehtestada tuleb asjakohased tegevuspõhimõtted ja kord tagamaks, et teenuse kasutajaid teavitatakse õigeaegselt ja usaldusväärselt kõigist muudatustest teenuse määratluses ja kõigis kohaldatavates tingimustes ning konkreetse teenuse privaatsuspõhimõtetes. 3. Kehtestada tuleb asjakohased tegevuspõhimõtted ja kord, mis võimaldavad teabenõuetele täielikult ja korrektselt vastata.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.4.3. Infoturbe haldus

Usaldusväärsuse tase	Vajalikud komponendid
Madal	Infoturvariskide haldamiseks ja juhtimiseks on olemas tõhus infoturbe halduse süsteem.
Märkimisväärne	Lisaks madalale tasemele peavad olema täidetud järgmised tingimused. Infoturbe halduse süsteem järgib infoturvariskide haldamise ja juhtimise juurdunud standardeid ja põhimõtteid.
Kõrge	Sama kui märkimisväärse taseme puhul.

2.4.4. Andmete säilitamine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Asjakohased andmed talletatakse ja neid säilitatakse, kasutades tõhusat teabehaldussüsteemi ning võttes arvesse andmekaitse ja andmete säilitamise suhtes kohaldatavaid õigusakte ja sellega seotud häid tavasid. 2. Andmeid säilitatakse, kuivõrd see on lubatud riigi õigusaktidega või muu riikliku halduskorraldusega, ja kaitstakse seni, kuni nad on vajalikud auditeerimiseks ja turvalisuse rikkumistega seotud uurimiste tarbeks ning säilitamiseks; pärast seda hävitatakse andmed turvaliselt.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.4.5. Ruumid ja personal

Järgmises tabelis on esitatud nõuded, millele peavad vastama ruumid ja personal ning vajaduse korral allhankijad, kes täidavad käesolevas määruses kirjeldatud ülesandeid. Iga nõude täitmine on proportsionaalne pakutava usaldusväärsuse tasemega seotud riski tasemega.

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Olemas on menetlused, millega tagatakse, et personal ja allhankijad on oma ülesannete täitmiseks piisavalt koolitatud, kvalifitseeritud ja kogenud. 2. Teenuse nõuetekohaseks käigushoidmiseks ja ressursside tagamiseks vastavalt selle põhimõtetele ja menetlustele on piisavalt töötajaid ja allhankijaid. 3. Teenuse osutamiseks kasutatavaid ruume jälgitakse pidevalt ja neid kaitstakse keskkonnasündmuste tekitatavate kahjude, ilma loata juurdepääsu ja muude asjaolude eest, mis võiksid mõjutada teenuse turvalisust. 4. Teenuse osutamiseks kasutatavates ruumides on tagatud, et juurdepääs aladele, kus hoitakse või töödeldakse isikuandmeid, krüptograafilisi andmeid või muid delikaatseid andmeid, on lubatud vaid volitatud töötajatele või allhankijatele.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.4.6. Tehniline kontroll

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Teenuste turvalisusega seotud riskide haldamiseks on olemas proportsionaalsed tehnilise kontrolli meetmed, mis kaitsevad töödeldava teabe konfidentsiaalsust, terviklust ja käideldavust. 2. Isikuandmete või delikaatse teabe vahetamiseks kasutatavad elektroonilise side kanalid on kaitstud pealtkuulamise, manipuleerimise ja taasesituse vastu. 3. Kui e-identimise vahendite väljastamiseks ja autentimiseks kasutatakse krüptograafiat, on juurdepääs tundlikele krüptograafiamaterjalidele vaid neil rollidel ja rakendustel, mille jaoks on juurdepääs vältimatult vajalik. Tagatakse, et selliseid materjale ei salvestata kunagi püsivalt lihttekstina. 4. Kasutatakse menetlusi, mis tagavad, et turvalisus säilib aja jooksul ning et olemas on suutlikkus reageerida riskitaseme muutumisele, intsidentidele ja turvalisuse rikkumistele. 5. Kõiki andmekandjaid, mis sisaldavad isikuandmeid, krüptoandmeid või muud delikaatset teavet, hoitakse ja transporditakse ning need hävitatakse ohutult ja turvaliselt.
Märkimisväärne	Lisaks madalale tasemele peavad olema täidetud järgmised tingimused. Kui e-identimise vahendite väljastamiseks ja autentimiseks kasutatakse krüptograafiat, on delikaatsed krüptomaterjalid manipuleerimise vastu kaitstud.
Kõrge	Sama kui märkimisväärse taseme puhul.

2.4.7. Nõuete järgimine ja auditeerimine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	Toimuvad korrapärased siseauditid, mis hõlmavad kõiki pakutavate teenuste osutamise seisukohast olulisi osi, et tagada asjakohaste põhimõtete järgimine.

Usaldusväärsuse tase	Vajalikud komponendid
Märkimisväärne	Toimuvad korrapärased sõltumatud sise- või välisauditid, mis hõlmavad kõiki pakutavate teenuste osutamise seisukohast olulisi osi, et tagada asjakohaste põhimõtete järgimine.
Kõrge	1. Toimuvad korrapärased sõltumatud välisauditid, mis hõlmavad kõiki pakutavate teenuste osutamise seisukohast olulisi osi, et tagada asjakohaste põhimõtete järgimine. 2. Kui süsteemi haldab otseselt valitsusasutus, auditeeritakse seda kooskõlas riigi õigusaktidega.