RIIGI INFOSÜSTEEMI AMET

Igor Taro
Siseministeerium
info@siseministeerium.ee

Teie 23.12.2025 nr 1-6/3351-1

Meie 20.01.2026 nr 1.1-20/262186

Arvamus IDTS muutmise seaduse eelnõu kohta

Austatud Igor Taro

Täname võimaluse eest esitada arvamus IDTS muutmise seaduse eelnõu ja selle seletuskirja kohta. Toetame innovatsiooni ja kaugtuvastuse kasutuselevõttu, kuid samas peame vajalikuks juhtida tähelepanu kriitilistele riskikohtadele, mis võivad mõjutada Eesti e-residendi elektroonilise identiteedi usaldustaset (LoA) ja turvalisust rahvusvahelisel tasandil.

Esitame järgmised ettepanekud:

1. ICAO dokumendi kiibi kontroll ja valideerimine

Eelnõus kirjeldatud kaugtuvastus toetub välisriigi ICAO reisidokumendi andmetele.

Ettepanek: Sätestada seaduse või rakendusakti tasandil kohustuslikud tehnilised kontrollid:

1) kiibi autentimine (*Active Authentication/Chip Authentication*) ja passiivne autentimine (PA);
2) ICAO dokumendi lost&stolen kontroll;
3) dokumendi väljaandja usaldusahela kontroll (BSI ja käsitsi lisamise protsess).

Põhjendus: ICAO dokumentide valideerimisel esineb sageli sertifikaatide vigu või puuduvad riikidevahelised usaldusahelad. Kui kiibi digitaalallkirja valideerimine ebaõnnestub, peab süsteem dokumendi tagasi lükkama, et tagada LoA "kõrge" tase.

2. Isikusamasuse kontroll ja vastendamine

Seletuskirjas kirjeldatud biomeetriline tuvastus on kriitiline dubleerivate identiteetide vältimiseks.

Ettepanek: Vajalik on kirjeldada meetmed, kuidas tehakse kindlaks, et isik mõlemal korral sama. Kas see toimub näiteks läbi asukohariigi isikukoodi? Millised meetmed on siis, kui isikukood puudub?

Tähelepanek: Kui e-residendil puudub asukohariigis isikukood või see on muutunud, peab riik tagama selge õigusliku aluse ja tehnilise võimekuse vastendada isik varasemate biomeetriliste

hõivetega ITDAK/ABIS süsteemis.

3. Järelevalve ja RIA rolli kajastamine

Seletuskiri keskendub peamiselt PPA ja SMIT koormusele, jättes tähelepanuta Riigi Infosüsteemi Ameti (RIA) rolli järelevalve ja eID skeemi tagatistaseme samaväärsuse hindamise otsustamisel.

Ettepanek: Täiendada seletuskirja peatükki 4.1, märkides, et seoses uue usaldusteenuse ja kaugtuvastuse meetodi lisandumisega suureneb oluliselt RIA järelevalvemaht (EUTS ja eIDAS tähenduses).

Põhjendus: Kuna tegemist on uue meetodiga (kaugtuvastus + usaldusteenus), peab RIA hakkama teostama järelevalvet uue skeemi ja selle osapoolte üle, et tagada vastavus eIDAS-e "kõrgele" usaldustasemele. See nõuab täiendavat ressurssi, mida seletuskirja finantsmõjude osas välja toodud ei ole.

4. Krüpteerimislahenduse funktsionaalsuse kaotamine

Seletuskirjas ei ole käsitletud asjaolu, et kaardivabale lahendusele üleminekul kaotavad e-residendid krüpteerimisvõimekuse.

Ettepanek: Täiendada eelnõu seletuskirja ja selgitada, et e-residendi eID vahend ei toeta krüpteerimist ning hinnata selle mõju kasutajagruppidele.

Põhjendus: Krüpteerimislahenduse funktsionaalsuse kaotamine on oluline muudatus kasutajatele, kes on harjunud dokumente konfidentsiaalsuse tagamiseks krüpteerima.

5. PPA roll eIDAS auditites

Seletuskiri jätab eksliku mulje, et PPA-l kaob kohustus osaleda eIDAS auditites.

Ettepanek: Korrigeerida seletuskirja, lähtudes asjaolust, et PPA peab jääma eIDAS auditi osapooleks, kuna vastutab esmase identiteedi loomise ja otsustusprotsessi eest.

Põhjendus: eIDAS-e usaldustaseme hindamine katab kogu väljastusahela, mitte ainult tehnilist teenusepakkujat. PPA osaleb eIDAS auditites osapoolena, kes vastutab esmase identiteedi kontrolli ja õiguse andmise protsessi eest, sõltumata sellest, et füüsilist kaarti enam ei väljastata.

6. Elusoleku kontroll ja andmete ajakohasus

E-residendi side asukohariigiga on dünaamiline, kuid Eesti registritel puudub otsene ligipääs välisriikide rahvastikuandmetele.

Ettepanek: Sätestada riskide maandamise meetmed e-residendi elusoleku ja tema andmete ajakohasuse kontrolliks (näiteks: mingi perioodilisusega biomeetria kontroll vms).

Põhjendus: Ilma regulaarse kontrollita (nn *liveness check* ja nimevahetuse kontroll) on kõrge risk, et eID vahend jääb kasutusse pärast isiku surma või andmete olulist muutumist, mida riik ei pruugi õigeaegselt tuvastada.

7. Seadmete turvalisus

Ettepanek: Määratleda selged tehnilised miinimumnõuded nutiseadmetele, mis tagavad turvalise kiibi lugemise ja biomeetria hõive, sealhulgas nõuded ekraanilukule ja juurdepääsupiirangutele (*anti-rooting*).

Põhjendus: E-residendi eID puhul liigub turvakriitiline funktsionaalsus riigi poolt kontrollitud kiipkaardilt kasutaja isiklikku nutiseadmesse. See tekitab järgmised riskid, mis vajavad maandamist:

1) **Vastavus eIDAS "kõrgele" tasemele:** eIDAS rakendusmäärus (EL) 2015/1502 nõuab, et "kõrge" usaldusväärsuse tasemega vahend peab olema kaitstud dubleerimise ja rünnete eest. Kui nutiseade on n-ö lahti murtud (*rooted* või *jailbroken*), on ründajal võimalik pääseda ligi rakenduse mälule ja kopeerida sealt identiteedi võtmeid. Ilma seadme terviklikkuse kontrollita ei ole võimalik tagada vahendi kopeerimiskindlust.
2) **Kasutaja kontroll seadme üle:** Ekraaniluku nõue on esmane kaitsemeede vältimaks identiteedi väärkasutust juhul, kui seade satub kolmandate isikute kätte. Kuna e-residendi eID-ga hakatakse tegema kõrge riskiga tehinguid (ettevõtete asutamine, pangaülekanded jms), on seadme füüsilise ja tarkvaralise turvakihi kontroll vältimatu osa usaldusahelast. Samuti vajab täpsemat selgitust see, kuidas kontrollitakse GPS emulatsiooni puudumist?
3) **Turvapaigad:** Seletuskirjas mainitud "uuendatud operatsioonisüsteem" on liiga ebamäärane mõiste. Tootjate toe lõppemine vanematele seadmetele tähendab, et neile ei väljastata enam kriitilisi turvapaiku, mistõttu võib identiteedi hõivamine toimuda seadme tasemel olemasolevate haavatavuste kaudu, ilma et kasutaja või teenusepakkuja seda märkaks. Vajalik on kirjeldada kontroll turvalise operatsioonisüsteemi osas.

8. Ettepanek sõnastada eelnõu punktis 41 toodud § 34^5 lõige 1 punkt 2 järgmiselt:
„2) *omab kehtivat e-identimise ja e-tehingute usaldusteenuste seaduses sätestatud otsust e-identimise süsteemi kõrge usaldusväärsuse taseme samaväärsuse vastavuse kohta;"*

9. Seletuskirjas on nimetatud riskide maandamise meetmena "e-residentsuse nõukoda”. Sellest tulenevalt teeme ettepaneku kaasata antud nõukoja koosseisu ka RIA eID valdkonna eksperdid.

10. Ühilduvuse tagamiseks eID ökosüsteemiga peab lahendus arvestama ettevõtlus- ja infotehnoloogiaministri 06.12.2021.a määrusega nr 72 „Tehnilised nõuded andmekandja kohta, millele võib kanda digitaalse dokumendi või dokumendi digitaalsed andmed“ ja Eesti e-identiteedi ökosüsteemiga (https://www.ria.ee/sites/default/files/documents/2025-10/eID-okosusteem-lisadega-2025.pdf)

Lugupidamisega

(allkirjastatud digitaalselt)

Joonas Heiter
peadirektor

Margus Reitalu
666 8879 margus.reitalu@ria.ee