



## POLITSEI- JA PIIRIVALVEAMET

Igor Taro  
Siseministeerium  
info@siseministeerium.ee

Teie 03.06.2026 nr 1-6/3482-1

Meie 18.06.2026 nr 1.2-4/136-2

Austatud siseminister

Olete 03.06.2026 edastanud Politsei- ja Piirivalveametile (PPA) kooskõlastamiseks siseministri määruse „Siseministri määruste muutmise seoses e-residentsuse programmi üleminekuga kaardivabale lahendusele“ eelnõu. Täname Teid sujuva protsessi ja PPA aktiivse kaasamise eest juba eelnõu ettevalmistamisel. Olles nimetatud eelnõu läbi töötanud, teeme allolevad ettepanekud.

1) Eelnõu Punktiga 7 lisatakse viide täiendavale standardile, millele sõrmejäljekujutis peab vastama. Teeme ettepaneku täiendada standardite loetelu viitega „või uuem“, mis tagab määrusega kooskõla ka juhul, kui vahepeal on avaldatud uuem standardi versioon.

2) Eelnõu punktiga 3 tunnistatakse kehtetuks määruse nr 56 § 1 lõige 11, mille kohaselt võib e-residendi digi-ID taotleja sõrmejäljed võtta dokumendi väljastamisel. Eelnõu seletuskirjas on öeldud, et e-residendi kaardivabale lahendusele üleminekul annab taotleja oma sõrmejäljed taotluse esitamisel kaugteel PPA biomeetrilise isiku tuvastamise ja isikusamasuse kontrollimise rakenduses. Selguse huvides täpsustame, et sõrmejälgi hakkab taotleja kaugteel andma juba varem, st alates 02.03.2027, kui võtame kasutusele biomeetrilise isiku tuvastamise ja isikusamasuse kontrollimise rakenduse.

3) Eelnõu seletuskirjas on mainitud, et nii pöidla kui ka väikese sõrme sõrmejäljed on tavaliselt halvema kvaliteediga, sest sõrmede asend ja kuju võivad takistada kontakti hõiveseadmega ning seetõttu ei pruugi võrdlustulemused olla piisavalt usaldusväärsed. Peame oluliseks täpsustada, et see kehtib just kaugteel, st mobiilse seadme kaudu sõrmejälgede andmise (pildistamise) puhul. Kontaktsete hõiveseadmete puhul saab pöidlalt vastupidi reeglina hea kvaliteediga sõrmejälje.

4) Seoses üleminekuga kaardivabale lahendusele teeme ettepaneku täiendada siseministri määruse nr 56 paragrahvi 17, lisades sätte, mille kohaselt „e-residendi digitaalse isikutunnistuse taotlusele lisatakse dokument taotleja välisriigis kriminaalkorras karistamise või karistuse puudumise kohta või tõend selle kohta, et sellist dokumenti ei ole taotlejal välisriigist võimalik saada“. Kuna kaardivaba lahenduse puhul ei pea e-residentsuse taotleja enam reeglina PPA või välisesinduse väljastuskohta kohale ilmuma, muutub teenuse kuritarvitamine distantstilt lihtsamaks. Vahetu inimkontakti kadumine võib hajutada ohumärke, mida on vaja potentsiaalsete pettuste ja väärkasutuse ennetamiseks.

Riski aitaks oluliselt maandada karistusregistri tõendi esitamise kohustuslikkus, nagu seda on soovitanud ka Riigikontroll juba oma 2020. aasta [auditi aruandes](#). Riigikontroll tuvastas auditi

käigus, et oleme valimisse jäänud perioodil väljastanud e-residendi digi-ID 48-le kriminaalkorras karistatud Soome kodanikule. Nendest veerandi puhul oli karistuseks määratud reaalne vanglakaristus ning viiendikul oli karistus majanduskuritegude eest. Seni oleme e-residenstsuse menetluse käigus küsinud karistusregistri tõendeid vajadus- ehk riskipõhiselt, kuid täna ei ole enam tegemist tõhusa meetmega. Tehisintellekti areng on muutnud e-residenstsuse taotleja vähem isikupäraseks, mis teeb kuritegelike motiivide (nt maksudest kõrvalehiilimise, rahapesu) tuvastamise aina keerulisemaks. Potentsiaalseid ohu- ja riskimärke on digitaalselt esitatavalt taotlusankeedilt aina keerulisem märgata. PPA ei ole valmis aktsepteerima riski, et ebapiisavate andmete tõttu saavad e-residendiks kriminaalkorras, sh majanduskuritegude eest süüdi mõistetud isikud. Kuna e-residenstsuse menetluse näol on tegemist haldusmenetlusega, siis ei saa karistuste andmeid kätte ka rahvusvahelise koostöö abil, kuna paljude riikide, sealhulgas näiteks Soome, siseriiklik õigus ei võimalda seda infot haldusmenetluse raames jagada.

Karistusregistri tõendi esitamise kohustuslikkus on PPA hinnangul äärmiselt vajalik meede, mida tuleb rakendada üleminekul kontaktivabale lahendusele. See aitab taastada osa „füüsilise kontrolli“ kihist, luues täiendava objektiivse ja kontrollitava signaali inimese tausta kohta.

5) Isikut tõendavate dokumentide andmekogu põhimääruse § 17 lg 2<sup>1</sup> sätestab, et logiandmeid säilitatakse kümme aastat toimumu tegemisest arvates. Tulenevalt eIDAS auditi tulemustest teeme ettepaneku muuta logiandmete säilitamise tähtaega – kümne aasta asemel kaksteist aastat.

#### eIDAS auditi leiu taust ja muudatuse vajadus

2026. aasta mai lõpus toimunud eIDAS auditi käigus tõi audiitor leiuna välja, et sündmuste logid ja tõendid sertifikaatide kasutustingimustega nõustumise kinnituse kohta peavad olema kättesaadavad ka 10-12 aasta pärast. eIDAS audiitori hinnangul tuleb arvestada asjaoluga, et tarkvara areneb iga paari aasta tagant, muutes rakendustaseme logid süsteemi migreerimise ajal vananenuks. Audiitor näeb siin õiguslikku riski, mistõttu on vaja logide säilitamist pikendada 10-lt aastalt 12-le aastale. See toimiks nii-öelda turvapuhvrina lisaks tavapärasele 10-aastasele piirangule, et katta tsiviilvastutust, seadusejärgseid aegumistähtaegu ja menetlusaega.

Tsiviilseadustiku üldosa seaduse (TsÜS § 146 lg 4) kohaselt on tahtliku rikkumise korral nõuete aegumistähtaeg 10 aastat. Kuna vaidlused võivad tekkida vahetult enne ja selle tähtaja piiril ja neile lisandub menetlusaeg, tagab 12-aastane logide puhver selle, et vajalikud tõendid ja logid (sertifikaatide kehtivusajad, sertifikaatide kasutustingimuste logid) on kohtuvaidluste tarbeks kättesaadavad. 12-aastane säilitustähtaeg tagab eIDAS määruse nõuetele vastavuse. See katab tahtliku rikkumise 10-aastase aegumistähtaja TsÜS alusel ning lisab 2-aastase puhvri võimalikeks kohtuvaidlusteks. Samal ajal maandatakse isikuandme kaitse riske, sest andmeid töödeldakse spetsiifiliselt õigusnõuete täitmiseks. Isikuandmete kaitse ja GDPR vaates saab andmete säilitamise õiguslikuks aluseks spetsiifiline juriidiline kohustus, mis välistab andmete kasutamise tavapäraseks äritegevuseks. Andmete algne kogumise eesmärk ehk teenuse osutamine lõpeb. eIDAS vaates tagab tehingute ja digitaalsete allkirjade tõendusväärtuse säilimine kogu vaidluse võimaliku elukaare vältel.

#### Õiguslik alus

Vaatavalt ETSI EN 319 411-1 (punkt OVR-6.4.6-01-) tuleb sertifikaatidega seotud sündmusi logida vähemalt 7 aastat pärast sertifikaadi kehtivuse lõppu. Kvalifitseeritud sertifikaadi maksimaalne kehtivusaeg on kuni 5 aastat. 7 aastat (nõutav logide säilitus) + 5 aastat

(sertifikaadi kehtivus) = 12 aastat mis tagab tõendite olemasolu sertifikaadi elutsükli lõpuni ning katab võimaliku kohtuvaidluse perioodi.

eIDAS audiitor tugineb pikema säilitusperioodi (12 aastat) nõude kehtestamisel otsekohalduvale eIDAS määrusele (Artikkel 24) ja selle aluseks olevale ETSI standardile (ETSI EN 319 411-1, OVR-6.4.6-01 ja REG-6.3.4-17), mis nõuab, et kasutustingimustega nõustumise logisid ja sertifikaadi andmeid säilitakse piisavalt kaua, et tagada teenuse vastavus ja toetada hilisemalt võimalikke juriidilisi vaidlusi. Kuigi ETSI EN 319 411-1 REG- 6.3.4-17 ja eIDAS konkreetset aastate arvu ei dikteeri, vaid nõuab vastavust kohalikule seadusandlusele, tuleneb see tavaliselt siseriiklikkust tsiviilõigusest ja lepingute aegumistähtaegadest. Siseriikliku õiguse kohandamisel toetutakse eIDAS-e üldisele nõudele säilitada infot nii kaua, kuni see on vajalik tõendite esitamiseks kohtus.

Lugupidamisega

(allkirjastatud digitaalselt)

Anita Preinvalts  
arendusosakond, identiteedi ja staatuste büroo  
teenuse omanik büroojuhi ülesannetes