

**Justiits- ja digiministri määruse „Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded autentimise ja digitaalse allkirjastamise teenuse tagamisel“ eelnõu
SELETUSKIRI**

1. Sissejuhatus

Määruses piiritletakse autentimise ja digitaalse allkirjastamise puhul osa, mida käsitletakse elutähtsa teenusena, mida osutab isikut tõendavate dokumentide seaduses sätestatud kvalifitseeritud usaldusteenuse osutaja. Lisaks nähakse ette nõuded elutähtsa teenuse toimepidevusele ja toimimisele ulatusliku katkestuse või selle ohu korral. Nõuete eesmärk on tagada riigi ja ühiskonna funktsioneerimise seisukohalt oluliste teenuste ning nende toimimist toetavate võtmetähtsusega teenuste toimimine ja töökindlus. Määrusega ei kehtestata võrreldes samasisulise kehtiv määrusega uusi nõudeid, siis ettevõtjate osas ei toimu halduskoormuses muudatusi.

Määrus kehtestatakse kriisiolukorra ja riigikaitse seaduse § 82 lõike 6 alusel. Määrusega asendatakse 1. oktoobril 2026 seoses kriisiolukorra ja riigikaitse seaduse jõustumisega kehtetuks muutuv ettevõtlus- ja infotehnoloogiaministri 11. jaanuari 2019. a määrus nr 4 „Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektroonilise isikutuvastamise ja digitaalse allkirjastamise tagamisel“ (edaspidi *määrus nr 4*).

Määruse eelnõu ja seletuskirja on koostanud Justiits- ja Digiministeeriumi riikliku IKT taristu talitus. Eelnõu keeletoimetuse on teinud sama ministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse toimetaja Inge Mehide (inge.mehide@justdigi.ee).

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb viiest paragrahvist.

Paragrahv 1 kirjeldatakse autentimise ja digitaalse allkirjastamise elutähtsat teenust (edaspidi koos *eID-teenus*). Arvesse on võetud teenuse iseärasusi, eelkõige teenuse lõppkasutaja jaoks enamasti tajumatut, kuid tehniliselt keerukat ülesannete jaotust nii avaliku kui ka erasektori osaliste vahel. eID-teenuse tervikuna kasutamiseks on vajalik seda võimaldavate dokumentide ja turvakoodide väljaandmine (vastutab Politsei- ja Piirivalveamet), ID-tarkvara toimimine, arendamine, haldamine ja klienditugi (vastutab Riigi Infosüsteemi Amet) ning kvalifitseeritud usaldusteenuse osutamine. Kvalifitseeritud usaldusteenuse all peetakse silmas isikut tõendavate dokumentide seaduse (edaspidi *ITDS*) alusel välja antud dokumentidele kantud sertifikaatide abil autentimise ja digitaalallkirja andmise võimaldamist ning sertifikaatide kehtivusinfo kättesaadavuse tagamist. Teisisõnu tuleb elutähtsa teenuse kirjelduse kehtestamisel lähtuda põhimõttest, et elutähtsa teenuse osutaja saab vastutada üksnes tema vastutusalasse kuuluvate teenusekomponentide toimepidevuse eest. Sellest põhimõttest ning termini „kvalifitseeritud usaldusteenus“ laiast tõlgendamisest lähtudes loetakse elutähtsaks teenuseks ITDS alusel välja antud dokumentidega elektroonilises keskkonnas isiku tõendamiseks, isikusamasuse kontrollimiseks (autentimiseks) ja digitaalallkirja andmiseks vajalike sertifikaatide kehtivusinfo kättesaadavuse tagamist.

Paragrahvis 2 sätestatakse kriisiolukorra ja riigikaitse seaduse (edaspidi *KORKS*) § 82 lõikele 9 tuginedes elutähtsale teenusele esitatavad nõuded. Samuti sätestatakse §-s 2 teenuse katkestuse maksimaalne lubatud aeg ja viidatakse teenuse taastamise korrale.

Lõikes 1 nähakse teenuseosutajale ette kohustus tagada elutähtsa teenuse toimimine vähemalt 361 kalendripäeval aastas.

Lõikes 2 määratakse kindlaks elutähtsa teenuse katkestuseks lubatud aeg ehk maksimaalne aeg, mille vältel võib teenus olla katkenud. Ajavahemiku piiritlemisel on arvestatud ID-kaardi ja mobiil-ID vahendusel osutatava teenuse kasutamisega seotud erisustega. Seetõttu on eelnõu kohaselt lubatud katkestuse aeg eID-teenuse puhul tööpäeviti vahemikus kell 9.00–18.00 kuni 45 minutit ja tööpäevaväliselt kuni kolm järjestikust tundi. Lõike teine lause täpsustab, et lubatud katkestuste summeeritud kestus peab võimaldama tagada teenuse toimimist § 2 lõikes 1 sätestatud mahus. Teisisõnu on lubatud teenuse katkestused üksnes nii pika aja vältel, et need ei takistaks teenuse osutamist § 2 lõikes 1 nõutud mahus. Kui korraldaval asutusel ei ole elutähtsa teenuse osutajalt olukorra kontrolli alt väljumise tõttu mõistlikult võimalik eeldada kohest teenuse taastamisega alustamist (näiteks üleriigiline pikaajaline elektrikatkestus, teenuseosutaja vastu suunatud füüsilised rünnakud jms), tuleks üldjuhul lubatud katkestuse aega hakata arvestama alates sellise olukorra lõppemisest (nt elektrivarustuse taastamine võrguettevõtja poolt, ettevõtte töötajate turvalisuse tagamine jms).

Paragrahvis 3 kirjeldatakse § 82 lõike 9 punkti 2 alusel nõudeid elutähtsa teenuse katkestuse ennetamiseks.

Lõikes 1 tuuakse välja loetelu ohtudest, millega peab teenuseosutaja elutähtsa teenuse toimimise tagamiseks ja katkestuse ennetamiseks riskianalüüsi koostades tingimata arvestama. Neljast punktist koosneva loetelu puhul ei ole tegemist täieliku ohtude ülevaatega, kuid riskianalüüsis peavad kajastuma vähemalt järgmised ohud:

- 1) andmesideteenuse katkestus;
- 2) elektrikatkestus;
- 3) võrgu- ja infosüsteemi vastu suunatud pahatahtlik tegevus;
- 4) oluline tehniline rike.

Lõige 2 koosneb kahest punktist, mille kohaselt kehtestatakse meetmed, mille rakendamine on elutähtsa teenuse toimepidevuse tagamiseks ja katkestuse ennetamiseks teenuseosutajale kohustuslik. Need on:

- sellise autonoomse elektritoitesüsteemi olemasolu, mis kindlustab elutähtsa teenuse osutamiseks vajalikele süsteemidele elektritoite vähemalt 24 tunniks;
- ühest kaablitrassist ja andmesideteenuse osutajast sõltumatu andmesideühenduse olemasolu.

Nõuete kehtestamisel on arvestatud, et elutähtsa teenuse osutajal oleks nende täitmiseks võimalik kasutada mistahes tehnoloogilisi lahendusi. Autonoomse elektritoitesüsteemi nõude korral võivad selleks peale diisलगeneraatori toel töötava elektritoitesüsteemi olla ka näiteks akud või patareisüsteemid ja taastuvenergia abil töötavad süsteemid. Analoogselt säilib elutähtsa teenuse osutajal võimalus oma parima teadmise juures otsustada ka dubleeritud andmesideühenduse tehnilise teostuse üle.

Paragrahvis 4 kirjeldatakse juhtumeid, mille esinemise korral loetakse olukord teenuse pikaajaliseks, raskete tagajärgedega või muu suure mõjuga katkestuseks. See tähendab, et autentimiseks ja digitaalallkirja andmiseks vajalike sertifikaatide kehtivusinfo kättesaadavuse tagamine on katkenud ning katkestus mõjutab samaaegselt olulist osa ITDSi alusel välja antud

autentimist ja digitaalset allkirjastamist võimaldavate dokumentide (sh mobiil-ID) kasutajatest. Need on juhtumid, kui:

- 1) elutähtis teenus on katkenud vähemalt 72 järjestikuse tunni vältel ning teenuse katkemine mõjutab sellel ajal 200 000 või enamat teenusekasutajat;
- 2) eID-teenuse katkestus põhjustab mõne teise elutähtsa teenuse pikaajalise, raskete tagajärgedega või muu suure mõjuga katkestuse.

Siinkohal on oluline märkida, et teenuse katkemise all ei peeta silmas olukordi, kus teenuse toimimine on peatatud riigi antud korralduse alusel või on katkenud mõni elutähtsa teenuse osutamiseks vajaliku sisendkomponendi toimimine, mille eest vastutab valitsusasutus (vastavalt Politsei- ja Piirivalveamet või Riigi Infosüsteemi Amet) (vt ka § 1 selgitust).

Paragrahvis 5 nähakse ette elutähtsa teenuse pikaajalisest, raskete tagajärgedega või muu suure mõjuga katkestusest või selle ohust teavitamise kord.

Lõike 1 kohaselt peab teenuseosutaja viivitamata teavitama elutähtsa teenuse pikaajalisest, raskete tagajärgedega või muu suure mõjuga katkestusest või selle ohust või elutähtsa teenuse toimepidevust oluliselt häirivast sündmusest või sellise sündmuse toimumise vahetust ohust Riigi Infosüsteemi Ametit kirjalikku taasesitamist võimaldavas vormis. Vorminõude kehtestamisel peeti silmas vajadust tõendada ja tuvastada intsidendi algust ja kulgu puudutava teabe liikumist. Teavitamiseks võib kasutada näiteks e-kirja, tekstisõnumit või spetsiaalset veebikeskkonda. Justiits- ja Digiministeerium on määranud elutähtsat teenust korraldavaks asutuseks Riigi Infosüsteemi Ameti kooskõlas KORKSi § 82 lõikega 4.

Lõike 2 kohaselt võib elutähtsa teenuse häirest või katkestusest teavitada ka mistahes muul viisil juhul, kui lõikes 1 nimetatud vorminõude järgimine ei ole olukorra ajakriitilisuse tõttu mõistlikult võimalik. Selline erisus on vajalik tagamaks, et tõsise intsidendi korral oleks teenuseosutajal võimalik kaasata formaalsete vorminõuete täitmise asemel maksimaalselt ressursse intsidendi lahendamisse. Siiski tuleb ka sellisel juhul esitada teade kirjalikku taasesitamist võimaldavas vormis hiljemalt 24 tundi pärast mistahes muus vormis esitatud teadet.

Lõikes 3 on loetletud asjaolud, mis peavad teates sisalduma. Sündmuse põhjuse loetelu koostamisel on lähtutud Euroopa Komisjoni juures tegutseva NISi (võrgu- ja infosüsteemide turvalisuse) koostöögrupi koostatud taksonoomiast (*root cause categories*). Esialgse teate esitamise ajal ei pruugi olla veel selge, mis intsidendi põhjustas ning kui paljusid inimesi juhtunu mõjutab. Esialgne teade on eeskätt mõeldud selleks, et viivitamata Riigi Infosüsteemi Ametile juhtunust võimalikult täpne ülevaade anda. Esialgne teade peaks sisaldama häire või katkestuse kohta vähemalt järgmist:

- 1) toimumise aeg ja hinnanguline kestus;
- 2) esialgne hinnang, kas katkestuse või häire põhjustas inimviga, süsteemitõrge, loodusõnnetus, pahatahtlik tegevus või kolmanda osapoole viga;
- 3) põhjuse kirjeldus;
- 4) esialgne hinnang mõju kohta teenuse terviklusele, käideldavusele ja konfidentsiaalsusele;
- 5) häire või katkestuse likvideerimiseks ning kahjuliku mõju vähendamiseks rakendatud ja rakendatavad meetmed;
- 6) esialgne hinnang mõju kohta teenuse kasutajale;
- 7) esialgne hinnang mõju kohta teiste elutähtsate teenuste toimepidevusele;
- 8) esialgne hinnang piiriülese mõju kohta

Lõike 4 kohaselt esitab teenuseosutaja Riigi Infosüsteemi Ameti nõudel kümne kalendripäeva jooksul raporti, mis sisaldab juhtunu kohta üksikasjalikumat teavet. Raport peab olema detailsem kui esialgne teade. Katkestuse põhjuse täpse kirjeldusena tuleks selgitada, mis täpsemalt intsidendi põhjustas. Näiteks ei piisa suure üldistusastmega „tehnilise rikke“ nimetamisest, vaid tuleb selgitada, kas tegemist oli tulekahju, veeavarii, administreerimisvea, küberründe, füüsilise ründe, riistvara rikke, elektrikatkestuse, andmesidekatkestuse või muuga ning milles intsident täpsemalt seisnes – kas teenus katkes, toimus andmeleke (kas lekkisid isikuandmed või muud konfidentsiaalsed andmed?), oli sissetungikatse (jõurünne, turvanõrkuse või konfiguratsioonivea ära kasutamine vms), kompromiteerimine (nt pahavara levitamine, kasutajakonto ülevõtmine, õngitsus) või pahavaraga (nt troojalase, lunavara, nuhkvaraga) nakatumine. Riigi Infosüsteemi Amet võib nõuda järgmise teabe esitamist:

- 1) häire või katkestuse alguse ja lõpu kuupäev ning kellaaeg;
- 2) mõjutatud kasutajate arv ning mõjutatud teenused ja infosüsteemid;
- 3) häire või katkestuse piiriülene mõju;
- 4) selgitus, kas häire või katkestuse põhjustas inimviga, süsteemitõrge, loodusõnnetus, pahatahtlik tegevus või kolmanda osapoolse viga;
- 5) häire või katkestuse põhjuse avastamise kuupäev, kellaaeg ja viis;
- 6) häire või katkestuse põhjuse kirjeldus ja häire või katkestuse kronoloogia;
- 7) mõju teenuse terviklusele, käideldavusele ja konfidentsiaalsusele;
- 8) rakendatud abinõud;
- 9) ülevaade senisest ja kavandatud kommunikatsioonist asutustele, kasutajatele ja avalikkusele.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu ei ole seotud Euroopa Liidu õigusega.

4. Määruse mõjud

Määrusega taaskeshtestatakse elutähtsa teenuse sisu autentimise ja digitaalse allkirjastamise tagamisel ning esitatakse teenuse toimepidevuse nõuded. Määruse alusel on elutähtsa teenuse osutaja kohustatud tagama elutähtsa teenuse samaväärselt määruses nr 4 sätestatuga. Samuti taaskeshtestatakse teenuse katkestuse lubatud aeg ning kriteeriumid, mille järgi on tegu elutähtsa teenuse ulatusliku või raskeid tagajärgi põhjustava katkestusega. Eelnõukohane määrus kirjeldab seega avalikkusele elutähtsa teenuse toimimise põhimõtteid ning elutähtsa teenuse osutaja kohustusi. Kuna määrusega ei tehta sisulisi muudatusi võrreldes määrusega nr 4, ei kaasne selle jõustumisega otsest mõju üheski mõjuvaldkonnas.

5. Määruse rakendamisega seotud tegevused ja kulud ning määruse rakendamise eeldatavad tulud

Määruse jõustumisega ei kaasne riigieelarvele otseseid ega kaudseid kulusid ega tõuse sellest tulu.

6. Määruse jõustumine

Eelnõukohane määrus jõustub üldises korras.

7. Eelnõu koostööstamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitatud Siseministeeriumile ja Riigi Infosüsteemi Ametile. Eelnõule esitatud tagasiside alusel on eelnõu ka muudetud.