Laura Kask, Kristiina Laanest

Elektroonilise allkirjastamise aja tuvastamine:

õiguslikud nõuded ja tehnilised võimalused

Käesolev artikkel on jätkuks Juridicas[*1] ilmunud artiklile, milles uuriti elektroonilise allkirja (edaspidi e-allkiri) tasemete eristamist Eesti õiguses vastavalt eIDAS-määrusele[*2], uutele nõuetele vastavate e-allkirjade kasutamist eraõiguslikes tehingutes ja haldusõiguslikes menetlustes ning elektrooniliste allkirjade piiriülest tunnustamist Euroopa Liidus. Vaatamata kehtivale üldisele vormivabaduse põhimõttele[*3] on tehinguid, mille kohustuslik vorminõue tuleneb seadusest. Samuti võib kokkuleppeliselt ette näha tehingute ja tahtevalduste kohustuslikud vorminõuded. Allkirja andmine võib olla vajalik nii füüsiliste kui ka elektrooniliste tahteavalduste esitamisel.

Eestis oli 2020. aasta maiks antud üle 960 miljoni digitaalallkirja[*4], seejuures on viimase kahe aasta jooksul antud kaks korda rohkem e-allkirju kui kogu varasema aja jooksul kokku[*5] ehk elektroonilisel teel tahteavalduste vahetamine ning lepingute sõlmimine on saanud nii avalikus- kui ka erasektoris igapäevaseks. E-allkirja andmise vahendina[*6] on Eestis kasutusel eelkõige Politsei- ja Piirivalveameti poolt isikut tõendavate dokumentide seaduse[*7] (ITDS) alusel väljastatud dokument (ID-kaart, e-residentsuse kaart, digi-ID, mobiil-ID, elamisloakaart), millega koos antakse välja elektrooniline dokument sellesse kantud digitaalset tuvastamist võimaldava sertifikaadiga ja digitaalset allkirjastamist võimaldava sertifikaadiga. Riiklikult väljastavate e-allkirja andmise vahendite kõrval kasutatakse järjest enam erasektori vahendeid (nt Smart-ID[*8]).

Artikli eesmärgiks on võrrelda allkirjastamist ja allkirjastamise aja kindlaksmääramist analoogmaailmas ja elektroonilises keskkonnas; vastata küsimusele, kuidas on võimalik e-allkirja seostada tehingu tegemise ajaga; milline on allkirjastamise aja õiguslik tähendus ja kuidas on see kehtivas õiguses reguleeritud. Artikli autorid on uurinud, millised riigisisesed nõuded on allkirjastamise ajale esitatud ning kuidas reguleerib allkirjastamise aega Euroopa Liidu õigus. Lisaks sellele kirjeldatakse e-allkirja tehnilist loomist, selgitamaks välja, milline e-allkirjastamise tarkvaras väljendatud aeg omab õiguslikku tähendust ning peaks olema käsitatav e-allkirjastamise ajana.

---

1 L. Kask. E- Eestist e-Euroopasse: elektrooniline allkiri riigisiseses ja piiriüleses suhtluses. – Juridica 2017/10, lk 675–686.

2 Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. – ELT L 257, 28.08.2014, lk 73–114.

3 Tsiviilseadustiku üldosa seadus (TsÜS), § 77 lg 3. – RT I 2002, 35, 216; RT I, 06.12.2018, 3.

4 ID-kaardi ja elektroonilise allkirja kasutamise statistika seisuga 12.05.2020. Arvutivõrgus: https://www.id.ee/ (12.05.2020).

5 2018. a jaanuari seisuga oli Eestis antud üle 450 miljoni digitaalallkirja. Arvutivõrgus: https://www.id.ee/ (28.05.2020). Vt ka L. Kask (viide 1), lk 685.

6 eIDAS-määruse art 3 p 22 kohaselt on e-allkirja andmise vahend seadistatud tark- või riistvara, mida kasutataks e-allkirja andmiseks.

7 RT I 1999, 25, 365; RT I, 31.01.2020, 14.

8 Alates 2018. a novembrist on Smart-ID tunnustatud kui kvalifitseeritud e-allkirja andmise vahend. Arvutivõrgus: https://www.smart-id.com/et/smart-id/ (28.05.2020).

1. Allkirjastamise aeg tahteavalduse ja tehingu tegemisel

1.1. Allkirjastamise aeg omakäelise allkirja andmisel

Tahteavalduse kaudu muudetakse isiku tahe teisele poolele nähtavaks ja õiguslikult siduvaks, s.t tahteavaldusega väljendatakse teatavate õiguslike tagajärgede kaasatoomise tahet. Tehing on TsÜS § 67 lõike 1 kohaselt toiming või omavahel seotud toimingute kogum, milles sisaldub kindla õigusliku tagajärje kaasatoomisele suunatud tahteavaldus. Tahteavaldust võib nimetada tehingu tuumaks, ilma milleta tehingut teha ei saa.[*9] Tehing võib sisaldada ka mitut tahteavaldust, mis on tehtud mitme isiku poolt. Tahteavalduse võib teha eelkõige mingi tegevusega, nagu näiteks testamendi tegemine, lepingu projekti saatmine, lepingust taganemise avalduse tegemine, ettepaneku esitamine lepingu muutmiseks[*10] või mingi muu toiming. Tahteavaldused peavad olema isikuga seotud ja seega kirjalikke tahteavaldusi allkirjastatakse sõltumata sellest, kas lepingule või tahteavaldusele on kirjaliku vormi nõue kehtestatud. Allkiri on ka üheks tahteavalduse lõpuleviimise väljendusvormiks, mille tulemusena arvatakse tehing kindla isiku poolt tehtuks. Seejuures peab isik mõistma, millega ta on nõustunud ja millele allkirja andnud ning milliseid tagajärgi tahteavalduse tegemine kaasa toob.

TsÜS § 77 lõikes 1 on kehtestatud tehingute vormivabadus koos õigusega seadusega või poolte kokkuleppel ette näha tehingutele kohaldatavad vorminõuded.[*11] Vormivabaduse põhimõttest hoolimata on õiguskäibes vaja arvestada tehingu sisu tõendamise hilisemate probleemidega.[*12] Kuigi kehtiv õigus ei defineeri tehingu vormi, on vorm tehingu väline avaldumisviis. Tehingu vormile seatavate nõuete peamisteks funktsioonideks on hoiatusfunktsioon (hoida ära liigset kiirustamist ja tehingu läbimõtlematut või kergekäelist tegemist), nõustamisfunktsioon (eelkõige juhul, kui kasutatakse nt notarit) ning tõendamisfunktsioon (tehingu tegemise fakti ja tehingu sisu hilisema kindlakstegemise ja tõendamise lihtsustamine).[*13] Allkirjastamine on aga tahte kinnitamine ning annab teisele lepingupoolele või kolmandatele isikutele lisakindluse, et isik on oma tegelikku tahet väljendanud. TsÜS kommentaaride autorid on möönnud, et omakäeline allkiri peab asetsema tehingudokumendi lõpus, millega see näitab ära tehingu sisu ulatuse, ja olema kirjutatud selliselt, et see võimaldaks identifitseerida allkirjastanud isikut. Allakirjutanu isiku identifitseerimiseks ei pea isik kirjutama oma täisnime, samuti ei pruugi isiku identifitseerimist välistada see, et ta on allkirja kirjutamisel teinud vea (nt jätnud ühe tähe välja). Piisav võib olla ka allkiri, mis on loetamatu, kuid on kirjutatud nii isikupäraselt, et selle võib kahtlusteta omistada konkreetsele isikule.[*14] Allkirjastamine annab infot selle kohta, et tahteavalduste esitamine on jõudnud lõplikusse faasi ehk pooled on saavutanud kokkuleppe või isikul on tekkinud veendumus tehingu tegemises ning selle väljenduseks antakse allkiri, mis on piisavalt isikupärane, võimaldamaks siduda tahteavaldus konkreetse isikuga.

TsÜS § 78 sätestab, et kui seaduses on sätestatud tehingu kirjalik vorm, peab tehingudokument olema tehingu teinud isikute poolt omakäeliselt allkirjastatud. Kuigi kirjaliku vorminõude tunnuseks on omakäeline allkirjastamine, ei ole omakäelist allkirjastamist seaduses defineeritud, samuti ei nähta ette omakäelise allkirja ning õigusliku jõu sidumist allkirjastamise aja märkimisega. See, millist tahet tahetakse kinnitada, tuleb iga kord eraldi tuvastada.[*15] Samas on erinorme, mille puhul on vorminõude täitmiseks oluline märkida omakäeliselt kirjutatud dokumendile ka kuupäev ja aasta. Näiteks tuleb pärimisseaduse[*16] § 24 lõike 1 kohaselt kodune testament kirjutada selle algusest lõpuni oma käega ja märkida ära testamendi tegemise kuupäev ja aasta ning omakäeliselt kirjutatud testamendile kirjutab testaator ise alla. Analoogmaailmas on omakäeliselt allkirjastatud tahteavalduse puhul allkirjastamise aeg tahte väljendamisega seoses oluline eelkõige siis, kui tehingu õiguslikud tagajärjed on seotud mingi ajavahemikuga. Aja märkimise kohustus võib olla ka pooltevaheline kokkulepe või tava, mida isikud peavad õiguslikult siduvaks.

9 P. Varul. Tahteavaldus ja selle tegemine. – Juridica 2010/7, lk 497.

10 Samas.

11 Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne. P. Varul, I. Kull, V. Kõve, M. Käerdi (koost.). Juura 2010, lk 243.

12 K. Sein. Tehingu vorminõuded ja nende järgimata jätmise tagajärjed. – Juridica 2010/7, lk 510.

13 Samas, lk 509.

14 Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne (viide 11), lk 248.

15 Lähemalt vt ka Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne (viide 11), lk 249.

16 RT I 2008, 7, 52, RT I, 10.03.2016, 16.

Samas ei pruugi tervikdokumendi allkirjastamine ja ka aja märkimine dokumendile iseenesest veel tähendada seda, et allkiri kinnitaks nõustumist kogu dokumendis kajastatud tingimustega. Näiteks on Riigikohus tsiviilasjas 3-2-1-144-09[*17] leidnud, et arve vastuvõtmine ja/või allkirjastamine ei tähenda üldjuhul seda, et arve vastuvõtja nõustub arvel esitatud tingimustega, milles varem kokkulepitud ei ole. Selleks et arvel näidatud tingimused muutuksid poolte kokkuleppe osaks, peaks olema arvel selgelt näidatud, et soovitakse kokku leppida seni kokku leppimata tingimustes. Seega ei ole ainuüksi dokumendi allkirjastamine piisav, et hinnata allkirja andnud isiku tegelikku tahet, vaid lisaks tuleb hinnata ka isiku käitumist, samuti tava ning varasemat poolte vahel väljakujunenud praktikat. Eelnevat kinnitab ka Riigikohtu seisukoht tsiviilasjas 2-17-14766, mille kohaselt ainuüksi see, et dokument on allkirjastatud hiljem, mitte lepingus märgitud ajal (intellektuaalne võltsimine), ei välista lepingust tulenevate õiguslike tagajärgede tekkimist.[*18]

Eelnevast ilmneb, et seaduses ei ole omakäelist allkirja defineeritud ega nõuta tehingute tegemisel reeglina ka allkirja andmise aja määramist. Seejuures ei pruugi allkirjastamise aeg tegelike õiguslike tagajärgede saabumise aspektist sugugi olla määrav. Samuti on Riigikohus oma praktikas seisukohal, et tsiviilõiguslikult ei ole oluline, millal dokument koostati, ja hilisem vormistamine ei välista õiguslike tagajärgede saabumist.

1.2. Allkirjastamise aeg e-allkirja andmisel

Kui analoogmaailmas kirjalikus vormis tehtud ja omakäelise allkirjaga kinnitatud tehingu kehtimiseks ei pea reeglina allkirjastamise aega tehingu tegemise ajaga seostama, siis kirjaliku vormiga võrdsustatud elektroonilise vormi puhul on allkirja ja tehingu seostamisele seatud lisatingimused. TsÜS § 80 kohaselt on elektrooniline vorm võrdne kirjaliku vormiga.[*19] TsÜS kommentaaride kohaselt ei ole elektrooniline vorm iseseisev tehingu vormi liik, vaid see asendab kirjalikku vormi, kui seadusest ei tulene teisiti, ning eeldab kolme tingimuse täitmist.[*20] Esiteks peab tehing olema tehtud püsivat taasesitamist võimaldaval viisil, teiseks sisaldama tehingu teinud isikute nimesid ja kolmandaks olema isikute poolt elektrooniliselt allkirjastatud (TsÜS § 80 lg 2). TsÜS § 80 lõike 3 kohaselt peab elektrooniline allkiri olema antud viisil, mis võimaldab allkirja seostada tehingu sisu, tehingu teinud isiku ja tehingu tegemise ajaga. Seega on elektroonilise allkirja kasutamisel tahteavalduse väljendamiseks oluline mitte ainult tehingu sisu ja isiku kindlakstegemine, nagu on üldnormina omakäelise allkirja puhul nõutud, vaid oluline komponent on ka allkirjastamise aeg.

Samas ei määra õigusaktid, millise ajaühiku puhul oleks täidetud tingimus, et elektroonilist allkirja peab olema võimalik seostada tehingu tegemise ajaga. Õigusaktid ei määra ka seda, milline e-allkirja andmiseks vajalik toiming[*21] tuleks siduda tehingu tegemise ajaga. Tehingu tegemise aega seadus ei defineeri, küll aga reguleerib TsÜS tähtaega. TsÜS § 134 lõike 2 kohaselt määratakse tähtaeg aastate, kuude, nädalate, päevade, tundide või väiksemate ajaühikute või kindlalt saabuva sündmusega. Sellest võiks lähtuda ka tehingu aja määramisel. Elektroonilise allkirja puhul tuleb arvestada tehingu aja määramisel, et aeg on allkirja konteineris esitatud sekundi täpsusega. Juriidiliste tagajärgede mõttes on küll võimalik, et tähtpäeva saabumine on määratud päevast väiksema ajaühikuga arvutatava tähtajaga (TsÜS § 136 lg 9), kuid sekundiga määratud tähtaega praktikas ei kasutata. Kuna tähtaja määramisel peetakse päevaks ajavahemikku kesköösti kesköösti (TsÜS § 136 lg 10), ei ole ka siin sekundid olulised, kuna minutid näitavad ära, kas tahteavaldus või dokument on esitatud tähtajaks.

Seega saab e-allkirja andmise aja kindlakstegemise ajaühiku tuletada seadusest, kuid e-allkirja andmise aja seostamine tehingu tegemise ajaga on jäetud praktika kujundada. Samuti ei ole omakäelise allkirja ja elektroonilise allkirja juriidiline tähendus erinev, sest ka elektroonilises keskkonnas dokumendi allkirjastamine pole piisav, et hinnata allkirja andnud isiku tegelikku tahet, vaid lisaks tuleb hinnata ka isiku käitumist, samuti tava ning varasemat poolte vahel väljakujunenud praktikat. Allkirjad erinevad tsiviilõiguslike nõuete puhul e-allkirja aja nõude poolest ning sellel peatutakse alljärgnevalt pikemalt.

17 RKTKo 17.12.2009, 3-2-1-144-09, p 11.

18 RKTKo 09.04.2020, 2-17-14766, p 15. Vt ka RKTKo 03.04.2019, 2-16-3785/114, p 14; RKTKo 23.10.2013, 3-2-1-96-13, p 34.

19 Lähemalt vt ka C. M. Laborde. Electronic Signatures in International Contracts. Frankfurt am Main: Peter Lang GMPH 2010, p 2017.

20 Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne (viide 11), lk 250–251.

21 E-allkirjastamise protsessi kirjeldust vt lähemalt: Kuidas allkirjastada ID-kaardiga dokumenti DigiDoc4 kliendis? Arvutivõrgus: https://www.id.ee/index.php?id=38801 (15.05.2020). E-allkirja andmiseks vajalikest toimingutest on täpsemalt juttu artikli kolmandas peatükis.

1.3. Allkirjastatud tahteavalduse tegemine ja kättesaamine

Selleks et teha kindlaks, milline on aja tähendus elektroonilises vormis tehtud tehingu puhul, tuleb analüüsida allkirjastatud tahteavalduse tegemist ja kättesaamist reguleerivaid norme, kuna õigusliku tähenduse omandab aeg alles tahteavalduse tegemisel ja kättetoimetamisel. Kuna tahteavaldusele kohaldatavad normid ei erista e-allkirja ja omakäelist allkirja, tekib küsimus, kas üldised tahteavalduse tegemise normid on kohaldatavad e-allkirjadele.

Tehingu tegemiseks on vajalik isiku tahteavaldus. TsÜS § 69 lõike 1 kohaselt peab kindlale isikule suunatud tahteavaldust tahteavalduse tegija väljendama ja see muutub kehtivaks kättesaamisega. TsÜS § 69 lõike 2 kohaselt on eemalviibijale tehtud tahteavaldus kätte saadud ja seega muutunud kehtivaks, kui see on jõudnud tahteavalduse saaja elu- või asukohta ja tahteavalduse adressaadil on mõistlik võimalus sellega tutvuda. Mõistlik võimalus tutvuda tähendab, et tahteavaldus on saabunud saaja mõjusfääri. Tahteavalduse sisust teadasaamise riski kannab tahteavalduse saaja. Tahteavalduse saatja peab vaidluse korral tõendama, et tahteavaldus on saaja mõjusfääri saabunud, v.a juhul, kui tegemist on TsÜS §-s 70 sätestatud teatega lepingu rikkumise kohta. Teade lepingu rikkumise kohta arvatakse kättesaaduks ajal, mil see tavaliste asjaolude korral oleks kätte saadud, kui saatja tõendab, et ta on tahteavaldust mõistlikul viisil väljendanud. Tahteavalduse saaja peab omakorda tõendama, et ta ei ole tahteavaldust kätte saanud.[*22]

Elektroonilise allkirja kasutamisel toimub tahteavalduse saatmine teisele poolele elektrooniliselt. Tahteavalduse jõudmist saaja mõjusfääri saab elektroonilise kanali kasutamise korral mõnevõrra lihtsamalt tõendada kui füüsilise kanali kasutamisel. Tänapäeval on võimalik kasutada väga erinevaid alternatiivseid saatmisvõimalusi, misläbi saab suurendada teabe kättetoimetamise efektiivsust. Selleks ei ole enam vaid e-maili teel manusena elektrooniliselt allkirjastatud tahteavalduste saatmine, vaid faile võib edastada ka pilveplatvorme (GoogleDrive, Dropbox jms) kasutades või suhtlusvõrgustike (Facebook, WhatsApp jms) kaudu. Kuigi Riigikohus on tsiviilasjas 3-2-1-123-07 käsitlenud, millal tuleb pidada e-kirja kättesaaduks, on aastate jooksul tekkinud tehniliste võimaluste juures küsitav, kas kättesaamise aega on igasuguste edastamisviiside puhul võimalik ühetaoliselt kirjeldada. Riigikohus on seisukohal, et teate e-kirjaga edastamise korral tuleb e-kiri arvata saajani jõudnuks, kui see on saabunud saaja või tema valitud teenusepakkuja serverisse. E-kirja tuleb aga pidada kättesaaduks TsÜS § 69 lõike 1 tähenduses alles siis, kui saajal on mõistlik võimalus sellega tutvuda. Millal on isikul mõistlik võimalus e-kirjaga tutvuda, sõltub konkreetsetest asjaoludest, sh sellest, kas saajal on interneti püsiühendus või mitte. Majandus- ja kutsetegevuses tuleb eeldada, et isik kontrollib e-posti vähemalt kord päevas. Seega saab majandus- ja kutsetegevuses pidada e-kirja kättesaaduks hiljemalt järgmisel päeval pärast e-kirja saabumist saaja või tema valitud teenusepakkuja serverisse.[*23] Eespool kirjeldatud seisukoht on avaldatud 2007. aastal, kuid see kehtib ka täna[*24], vaatamata sellele, et interneti kasutatavus ning võimalus oma e-kirjadele ligi pääseda on suurenenud ning saaja või teenusepakkuja serverisse jõuab e-kiri murdosa sekundiga. Seega puudub tehnoloogiline põhjus ja vajadus revideerida Riigikohtu seisukohta, mille kohaselt tuleks tahteavaldus, mis edastatakse e-kirjaga, arvata kättesaaduks järgmisest päevast pärast e-kirja saabumist. Samas võimaldavad mitmed suhtluskeskkonnad (Messenger, WhatsApp), mille kaudu on võimalik ka dokumente vahetada, näha, millal adressaat on talle saadetud teate avanud. Näiteks kuvab Messenger sõnumi lugemise aja, WhatsApp näitab, kas faili või sõnumit on vaadatud. Autorid leiavad, et kui see on pooltevahelises suhtluses tavapärane ja tehingu sisu nõuab viivitamatut kättetoimetamist, võib uudsete tehnoloogiliste lahenduste kaudu edastatud tahteavalduse puhul kättesaamise ehk saaja mõjusfääri jõudmise aega kokkuleppeliselt määrata. Näiteks võivad pooled selliste tehniliste lahenduste puhul, mis võimaldavad tuvastada aega, millal isik on sõnumi avanud, või mis fikseerivad ka saatmise aja, tahteavalduse kättesaamise siduda sõnumi lugemise ajaga.[*25] Samas tuleb

22 P. Varul (viide 9), lk 503.

23 RKTKo 21.12.2007, 3-2-1-123-07, p 12. Mõnevõrra teistsugune reegel tuleneb ühtse tugiraamistiku kavandi (DCFR) art I.-1:109 lg 4 p-st d, mille kohaselt arvatakse elektrooniliselt saadetud teade kättesaaduks, kui saajal on sellele juurdepääs olemas, seega kui e-kiri on jõudnud saaja serverisse, vt ka UNCITRAL Model Law on Electronic Commerce, 1996, art 15 lg 2. – UNIDROIT Principles. Rome 2004, lk 29).

24 Seadusandja on kehtestanud erandid teabe kättetoimetatuks arvamise üldreeglist. Näiteks tsiviilkohtumenetluse seadustiku (TsMS; RT I 2005, 26, 197; RT I, 19.03.2019, 23) § 314[1] lg 1 kohaselt peetakse sidevahendit kasutades saadetud menetlusdokument kättetoimetatuks kolme tööpäeva möödumisel saatmisest arvates.

25 Alates 01.01.2013 on kohtutel õigus võtta kostjatega ühendust ka näiteks Facebooki kaudu, selline võimalus peaks aitama kaasa menetluse kiirendamisele. Dokumente ei saa pidada küll kättetoimetatuks, kuid Facebooki kontole on võimalik saata teavitus dokumentide teatavakstegemise kohta. Täpsemalt vt M. Teder. Kohtud võivad inimeste leidmiseks ka sotsiaal-

tüüplepingute puhul järgida võlaõigusseaduse[*26] (VÕS) § 42 lõike 3 punkti 35, mille kohaselt tahteavalduse kättesaaduks arvamise reguleerimine erinevalt seaduses sätestatust on tüüptingimusena ebamõistlikult kahjustav ja tühine. Ilmselt ei välista see tahteavalduse tegemise aja kokkuleppimist.[*27]

Kuigi tehnoloogia võimaldab välja selgitada tahteavalduse kättesaamise aja ning pooltel on võimalik kokku leppida tahteavalduse kellaajalises kättesaamises, siis kindlasti tuleks arvestada ka tehnilist võimekust ja mõistlikkuse põhimõtet, et sisustada elektroonilise allkirjaga väljendatud tahteavalduse kättesaamise aeg. Elektroonilises keskkonnas saabunud tahteavalduse sisuga tutvumine võib olla raskendatud tehnilise võimekuse puudumise tõttu. Näiteks e-allkirja kehtivust saab kontrollida spetsiaalse tarkvara abil, kuid tarkvara ise võib olla riigiti mõnevõrra erineva ülesehitusega. Hinnates mõistlikku võimalust tahteavaldusega tutvumiseks[*28], tuleb arvestada seega ka tehnilise võimekuse loomiseks vajaminevat aega ning isiku enda tehnilist taiplikkust selliste e-allkirjadega toimetulemiseks.

Eeltoodust saab järeldada, et analoogmaailmas ja elektroonilises keskkonnas edastatud allkirjastatud tahteavalduse tegemise ning kättesaamise õiguslikud nõuded ei erine. Elektrooniliselt edastatud tahteavalduse puhul loovad tehnilised vahendid paremad võimalused nii allkirjastatud kui ka allkirjastamata tahteavalduse kättesaamise kontrolliks.

2. Nõuded omakäelise allkirjaga võrdväärsele e-allkirjale Euroopa Liidu õiguses

Ka Euroopa Liidu õiguses ei ole allkirjastamise aja mõistet sisustatud. Enne eIDAS-määruse jõustumist Eestis erinevate tasemetega e-allkirju ei eristatud ning tinglikult võis allkirju jagada digitaalallkirjaks ja muudeks elektroonilises vormis allkirjadeks. TsÜS § 80 lõike 3 kohaselt peetakse e-allkirjaks ka digitaalallkirja, mis hõlmab erinevaid eIDAS-määruses sätestatud allkirja tasemeid.[*29] Käesolev artikkel keskendub eIDAS-määruse elektroonilise allkirja normidele, mis käsitlevad omakäelise allkirjaga võrdväärset e-allkirja ehk kvalifitseeritud e-allkirja.

eIDAS-määruse artikli 3 lõike 12 kohaselt on kvalifitseeritud e-allkiri täiustatud e-allkiri, mis antakse kvalifitseeritud e-allkirja andmise vahendi abil ja mis põhineb e-allkirja kvalifitseeritud sertifikaadil. Vastavalt eIDAS-määrusele on kvalifitseeritud e-allkiri võrdväärne omakäelise allkirjaga (art 25 lg 2). Omakäelise allkirjaga võrdväärne elektrooniline allkiri on seega elektrooniline allkiri, mis

- vastab täiustatud e-allkirja nõuetele (eIDAS-määruse art 26) ehk allkiri on seotud ainuüksi allkirja andjaga, allkirja abil on võimalik allkirja andjat tuvastada, allkiri antakse e-allkirja andmiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures kasutada üksnes allkirja andja, ning allkiri on allkirjastatud andmetega seotud sellisel viisil, et kõik hilisemad andmete muudatused on võimalik tuvastada;
- kasutab allkirja loomisel kvalifitseeritud e-allkirja andmise vahendit. Näiteks peab allkirja andmiseks kasutatav kiip olema sertifitseeritud eIDAS-määruse artikli 30 kohaselt;
- põhineb e-allkirja kvalifitseeritud sertifikaadil ehk peab vastama eIDAS-määruse artiklis 28 toodud nõuetele.

Kuna määrus on vahetult kohaldatav, ei ole liikmesriigi õigusaktis võimalik omakäelise allkirjaga võrdväärse elektroonilise allkirjana määratleda elektroonilist allkirja, mis ei vasta eIDAS-määruses kvalifitseeritud e-allkirjale sätestatud nõuetele. eIDAS-määruses toodud üldpõhimõte loob õigusliku aluse ka piiriüleseks e-allkirjade tunnustamiseks avalikus sektoris. Kui liikmesriik nõuab avaliku sektori asutuse poolt või selle

võrgustikke kasutada. – Postimees, 02.01.2013. Arvutivõrgus: https://www.postimees.ee/1090258/kohtud-voivad-inimeste-leidmiseks-ka-sotsiaalvorgustikke-kasutada (15.05.2020).

26 RT I 2001, 81, 487; RT I, 08.01.2020, 10.

27 Riigikohus on tsiviilasjas 3-2-1-151-11 leidnud, „et lepingus, mille teiseks pooleks on tarbija, on ebamõistlikult kahjustav eelkõige tüüptingimus, millega nähakse ette tahteavalduse teatavaks tegemine erinevalt seaduses sätestatust ja see on teisele lepingupoolele kahjulik, välja arvatud juhul, kui erisus käib teise lepingupoole tahteavalduse vormi kohta või kui nähakse ette, et tingimuse kasutaja võib lugeda teise lepingupoole poolt tingimuse kasutajale antud aadressi õigeks niikaua, kuni talle ei ole teatatud teist aadressi“, vt RKTKo 25.04.2012, 3-2-1-151-11, p 12.

28 Mõistlikkuse hindamisel arvestatakse VÕS § 7 lg 2 kohaselt võlasuhte olemust ja tehingu eesmärki, tegevus- või kutseala tavasid ja praktikat, samuti muid asjaolusid.

29 E-allkirja tasemete kohta loe lähemalt: L. Kask (viide 1).

nimel osutatava internetipõhise teenuse kasutamiseks kindlal tasemel e-allkirja, peab riik tunnustama ka teiste riikide ja teenusepakkujate vahendeid kasutades antud e-allkirju, mis on määruses sätestatud formaadis või antud määruse rakendusaktides määratud meetodeid kasutades (art 27 lg 2). eIDAS-määruse rakendamiseks on loodud ka rakendusaktid, millest e-allkirju käsitlev rakendusakt[*30] viitab standarditele, millele vastavaid e-allkirju peavad Euroopa Liidu liikmesriigid olema võimelised käsitlema. Standarditele mitte vastavate e-allkirjade puhul jääb nende menetlemise piiriülese võimekuse tagamine allkirja looja riigile.[*31]

Seega ei kohusta Euroopa õigusaktid omakäelise allkirjaga võrdväärse elektroonilise allkirja ehk kvalifitseeritud e-allkirja puhul allkirjastamise aega määrama. Siiski ei saa asuda seisukohale, et allkirja andmise aja fikseerimine oleks vastuolus eIDAS-määrusega, kuna kvalifitseeritud e-allkirja puhul on üheks nõudeks, et allkiri on allkirjastatud andmetega seotud sellisel viisil, et kõik hilisemad andmete muudatused on võimalik tuvastada. Nõudest saab autorite hinnangul lugeda kaudselt välja ka allkirjastamisel mingi ajakomponendi fikseerimise, millest edasised muudatused tuleb fikseerida. Riigisiseselt tuleneb allkirjastamise aja kindlaksmääramise kohustus TsÜS § 80 lõikest 3. Samas ei määratle eIDAS-määrus ega riigisisene õigus, mida pidada allkirjastamise ajaks.

3. Omakäelise allkirjaga võrdväärse e-allkirja tehnilised komponendid

3.1. Omakäelise allkirjaga võrdväärse e-allkirja tehniline loomine

Selleks et hinnata, milline e-allkirja andmiseks vajalik toiming tuleks siduda tehingu tegemise ajaga, tuleb kirjeldada e-allkirja loomisel kasutatavaid tehnilisi komponente.

Kvalifitseeritud e-allkirja tehnilisel loomisel juhindutakse lisaks eIDAS-määrusest tulenevatele nõuetele ja tehingute tegemist reguleerivatele kehtivatele õigusaktidele ka mitmest rahvusvahelisest standardist. Rahvusvaheliste standardite rakendamisega tagatakse e-allkirja loomise komponentide vastavus eIDAS-määruses sätestatud nõuetele ning usaldusteenuste turvalisuse ja koosvõime kõrge tase. Omakäelise allkirjaga võrdväärse e-allkirja loomise komponentide võtmes on kesksel kohal eIDAS-määruse rakendusaktis[*32] tunnustatud Euroopa Telekommunikatsioonistandardite Instituudi (ETSI) standardid. Eestis on valdavalt kasutusel ETSI standarditele vastavad XAdES-vormis e-allkirjad ja ASiC-tüüpi e-allkirjade konteinerid, kuid e-allkirjade eri formaatide ülesehituse loogika on analoogne.[*33]

E-allkirja andmise ajahetke kindlakstegemise seisukohast on kohane eristada kolme e-allkirja komponendi ajamärget:

- e-allkirja andmise vahendi, näiteks arvuti või teenusepakkuja serveri fikseeritud aeg (ingl *Claimed Time*),
- usaldusteenuse osutajalt saadud e-allkirja ajatempli (ingl *Time Stamp*) aeg ning
- e-allkirja sertifikaadi kehtivuskinnituse (ingl *Online Certificate Status Protocol*) päringu aeg.

Nimetatud e-allkirja komponentidega seotud ajamärked on isikule nähtavad DigiDoc-tarkvara[*34] kaudu.

---

30 Komisjoni rakendusotsus (EL) 2015/1506, 8. september 2015, millega kehtestatakse täiustatud e-allkirja ja täiustatud e-templi vormingu kirjeldus vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 27 lõikele 5 ja artikli 37 lõikele 5. – ELT L 235, 09.09.2015, lk 37–41. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006 (15.05.2020).

31 M. Erlich. E-allkirjad Euroopas ja nende käsitlemine Eestis. Juhend ja nõuanded e-allkirjade käsitlemiseks. Arvutivõrgus: https://www.ria.ee/public/PKI/EL_e-allkirjade_kasitlemine.pdf (15.05.2020).

32 Komisjoni rakendusotsus 2015/1506 (viide 30), mille kohaselt peavad art-s 1 nimetatud täiustatud e-allkirjad vastama ühele otsuses nimetatud ETSI tehnilistest kirjeldustest.

33 Electronic Signatures and Infrastructures (ESI). XAdES digital signatures. Part 1: Building blocks and XAdES baseline signatures. ETSI EN 319 132-1 V1.1.1 (2016-04). Arvutivõrgus: https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf (08.05.2020); Electronic Signatures and Infrastructures (ESI). Associated Signature Containers (ASiC). Part 1: Building blocks and ASiC baseline containers. ETSI EN 319 162-1 V1.1.1 (2016-04). Arvutivõrgus: https://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf (08.05.2020). Lisaks DigiDoc-tarkvarale on komponendid nähtavad ka alternatiivsete e-allkirja valideerimise rakenduste kaudu.

34 DigiDoc-tarkvara võimaldab avada digitaalselt allkirjastatud dokumente, kontrollida allkirjade kehtivust, digitaalselt allkirjastada ja andmeid krüpteerida, vt Digidoc tarkvara. Riigi Infosüsteemi Amet. Arvutivõrgus: https://www.ria.ee/et/riigi-infosusteem/eid/digidoc-tarkvara.html (09.05.2020).

Esimene ajakomponent on isiku poolt e-allkirjastamisel kasutatud vahendi või teenusepakkuja serveri fikseeritud aeg, mis on seadme või serveri ajaks e-allkirjastamise (PIN2 ehk e-allkirjastamise PIN-i sisestamise) hetkel pandud. Tehniliselt on tegemist vahendi poolt määratud ajahetkega, millal allkirjastaja n-ö väidab, et ta on e-allkirja andnud.[*35] E-allkirja andmise vahendi või teenusepakkuja serveri poolt fikseeritud aeg salvestatakse PIN2 ehk allkirjastamise PIN-i sisestamisel e-allkirja konteinerisse ning selliselt moodustatud baasallkirja ei ole võimalik hiljem muuta ilma allkirjastamise tehnilist ahelat kahjustamata. Siinkohal tuleb kohe arvestada ka võimalusega, et e-allkirja andmise vahendi fikseeritud aeg ei pruugi olla täpne. Oma seadme aega saab muuta isik manuaalselt ise, samuti võivad seadme aja täpsust mõjutada välised faktorid isiku teadmata. E-allkirja andmise vahendi aja fikseerimist võiks eelkõige võrrelda isiku poolt kuupäeva märkimisega allkirjastatavale dokumendile: märgitud kuupäev võib langeda kokku allkirjastamise ajaga, kuid ei pruugi.

Teine ajakomponent on vahetult pärast allkirjastaja poolt PIN2 sisestamist sooritatav ajatemplipäring usaldusteenuse osutajale.[*36] Ajatempliga toimub allkirjastamise elektrooniliste andmete seostamine kindla ajahetkega, et tõendada tehingu ja e-allkirja andmete olemasolu ajatemplipäringu tegemise ajahetkel. Ajatemplit võib võrrelda analoogmaailmas ümbrikuga, mille sees on teave ja mille peal on pitsat ajaga, millal need andmed ümbrikusse pandi, kuid sellega ei saa tõendada, millal teave ise dokumenteeriti. Kuigi Eesti praktikas võrdsustatakse ajatemplipäringu aeg allkirja andmise ajaga, tuleb arvestada, et ajatemplipäringuga ei saa kontrollida, milline maailmaaeg[*37] eksisteeris sel hetkel, kui isik PIN2 sisestamisega oma tahteavalduse kinnitas. Ajatemplipäringuga fikseeritakse tegeliku maailmaaja täpsusega ajahetk, millele eelnev sündmus – baasallkirja andmine – on aga juba toimunud.[*38]

Kolmandaks, kuivõrd kvalifitseeritud e-allkiri on kehtiv ainult siis, kui selle andmise hetkel e-allkirja kvalifitseeritud sertifikaat kehtib, tehakse sertifikaadi kehtivuse kontrollimiseks pärast ajatemplipäringut kehtivuskinnituse päring usaldusteenuse osutajale. Kehtivuskinnituse päring võimaldab küsida infot sertifikaatide kehtivuse kohta reaalajas. Seega ei kontrollita kehtivuskinnituse päringu tegemisel tagasiulatuvalt, kas e-allkirja andmise vahendi poolt fikseeritud ajal või ajatemplipäringu ajal sertifikaat kehtis, vaid päring näitab sertifikaadi kehtivust päringu tegemise ajahetkel.[*39] Täiendava tehnilise kontrolli meetmena võrdleb Digidoc-tarkvara e-allkirja andmise vahendi ja kehtivuskinnituse päringu kaudu saadud ajahetke kokkulangevust. Kui ajaline erinevus on üle 15 minuti, katkeb allkirja moodustamise ahel ning kvalifitseeritud e-allkirja konteinerit lõpuni luua ei saa.

Eestis kasutatakse e-allkirja loomisel kõiki kolme komponenti just sellises järjestuses ja kõigi kolme komponendi ajamärked on samas ajalises järjestuses salvestatud ka e-allkirja konteinerisse. Eesti Digidoc-tarkvara kuvab e-allkirja konteineri avavaates e-allkirja andmise ajana ajatemplipäringu aja, e-allkirja konteineri detailvaates on aga näha kõik kolm aega. Kuna ajatemplipäring ja kehtivuskinnituspäring tehakse Eesti parima praktika kohaselt vahetult pärast e-allkirja andmise seadmesse PIN2 sisestamist ning ajatemplipäringu ja sertifikaadi kehtivuskinnituse päringu vahe ei või olla enam kui 15 minutit[*40], jääb üldjuhul kõigi kolme komponendi aeg ühte kuupäeva, mistõttu allkirja andmise kuupäeva üle vaidlusi enamasti ei esine.

Siiski on juba moodustatud e-allkirja puhul võimalik teha ajatemplipäring ja kehtivuskinnituse päring hiljem uuesti, misjärel uuenevad ka e-allkirja konteinerisse kantud ajamärked.[*41] E-allkirja andmise seadme määratud aeg jääb aga seejuures samaks. Praegu ei ole aga käesoleva artikli autoritele teada, et keegi väljaspool teoreetilisi uuringuid e-allkirja uue ajatemplipäringuga või kehtivuskinnituse päringuga oleks moonu-

35 ETSI standardis kirjeldatakse e-allkirja andmise vahendi poolt fikseeritud aega järgmiselt: "The SigningTime qualifying property's value shall specify the time at which the signer claims to having performed the signing process." Vt Electronic Signatures and Infrastructures (ESI). XAdES digital signatures (viide 33), lk 25.

36 Varasemate TimeMark-tüüpi allkirjade puhul on ajatemplipäring kokku viidud kehtivuskinnituse päringuga.

37 Maailmaaja kohta täpsemalt vt https://et.wikipedia.org/wiki/Maailmaaeg (15.05.2020).

38 Samamoodi defineeritakse ajatemplipäringut ka ETSI standardis: "Electronic time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time. […] Containers for electronic time-stamps proving that some or all the signed data objects have been created before certain time instant." Vt Electronic Signatures and Infrastructures (ESI). XAdES digital signatures (viide 33), p 5.3.

39 Sertifikaatide peatamise skeemi tõttu ei ole võimalik kehtivuskinnituse päringu kaudu saada informatsiooni, kas sertifikaat kehtis mingil kindlal ajahetkel kunagi minevikus.

40 Kindlustamaks, et allkirjastamisel sertifikaat kehtib, on Eesti praktikas ajatemplipäringu ja sertifikaadi kehtivuskinnituse päringu vaheline aeg piiratud 15-minutiga.

41 T. Mets, A. Paršovs. Time of Signing in the Estonian Digital Signature Scheme. – Digital Evidence and Electronic Signature Law Review 2019, lk 44.

tanud tehingu tegelikke asjaolusid ning et see oleks kaasa toonud õigusvaidlusi. Ühtlasi puudub sellel artikli autorite hinnangul praktiline väärtus, sest mitmepoolse tehingu korral saab tahteavalduse esitaja tõendada tema enda valduses oleva e-allkirja konteineri abil, millal päring tegelikult tehti, lisaks on tahteavalduse esitamisel elektroonilises keskkonnas alati vajalik mingi kandja või kanali kasutamine, et tahteavaldus kätte toimetada. Kui aga tahteavalduse esitajal ei ole säilinud e-allkirja esialgset konteinerit, on võimalik vajalikke andmeid küsida usaldusteenuse osutajalt, kellel on ajatemplipäringu ja kehtivuskinnituse päringu andmete säilitamise kohustus. E-identimise ja e-tehingute usaldusteenuste seaduse*[42] (EUTS) § 5 lõike 3 kohaselt kohustub kvalifitseeritud usaldusteenuse osutaja dokumenteerima usaldusteenuse osutamisel tehtud toimingud ning säilitama sellekohast tegevuslogi kümme aastat kirje loomisest arvates. Oluline on siinkohal mõista, et hilisema päringuga ei saa e-allkirja konteineris olevat ajatemplipäringu aega muuta esialgsest varasemaks, vaid sellega fikseeritakse uue päringu ajahetk.

3.2. Omakäelise allkirjaga võrdväärse e-allkirja seostamine tehingu tegemise ajaga

E-allkirja aja seostamise nõue tuleneb TsÜS § 80 lõikest 3, mida on eespool käsitletud. Eespool kirjeldatud kolme ajakomponendi puhul tuleb eristada, kuidas neid siduda tehingu tegemise ajaga. Hetkel, kui isik e-allkirjastamisel PIN2 sisestab ja fikseeritakse e-allkirja andmise vahendi määratud aeg, tekib muutumatu ja terviklik ahel, mis seob omavahel allkirjastaja isiku, allkirjastamisel kasutatud vahendi poolt talletatud aja ja tehingu sisu. Juriidiliselt vastab selline e-allkiri TsÜS § 80 lõigetes 2–3 sätestatud tehingu elektroonilise vormi tingimustele (jättes reservatsiooni, et e-allkirja andmise vahendi poolt fikseeritud aeg ei pruugi olla siiski täpne). Põhjusel, et e-allkirja andmise vahendi aega ei saa pidada usaldusväärseks, rakendataksegi Eestis praktikat, mille kohaselt peetakse kvalifitseeritud e-allkirja andmise ajaks hoopis ajatemplipäringu tegemise aeg. Ajatemplipäringu aeg vastab tegelikule maailmaajale, millal tehingu ja e-allkirja andmete olemasolu on tõendatud.

Alternatiivselt on võimalik kaaluda e-allkirja andmise ajana ka e-allkirja kvalifitseeritud sertifikaadi kehtivuskinnituse päringu tegemise aega, sest selleks hetkeks on lisaks ajatemplile olemas ka veendumus sertifikaadi kehtivuse osas. Kuigi sertifikaadi kehtivuskinnituse päring etendab keskset rolli kvalifitseeritud e-allkirja kehtivuse puhul, on käesoleva artikli autorite hinnangul kehtivuskinnituse päring oluline, tõendamaks, et sertifikaat kehtib ja antud e-allkiri vastab kvalifitseeritud e-allkirja tingimustele, kuid seda ei peaks käsitama e-allkirja andmise ajana.

Eelnevast järeldub, et e-allkirja andmise toimingu sidumine tehingu tegemise ajaga TsÜS § 80 lõike 3 tähenduses on problemaatiline ja eeldab konsensust. Lahendusvõimaluste otsimist raskendab tõik, et seadusandja tahe e-allkirja sidumisel tehingu tegemise ajaga on sisult ebaselge. Eelkõige tekitab küsimusi, millise komponendi fikseeritud ajahetk ning millisel moel, arvestades ka e-allkirja eri tasemeid, peab olema tehingu tegemise ajaga seostatud.

E-allkirja andmise aja sidumine tehingu tegemise ajaga on omakäelise allkirjaga võrdväärse e-allkirja puhul olnud pikalt Eesti praktikas lähtekohaks. Seetõttu ei ole õiguskindluse, aga ka tehingukäibe usaldusväärsuse seisukohast käesoleva artikli autorite hinnangul otstarbekas e-allkirja andmise aja fikseerimisest üldse loobuda. Ühe võimalusena võiks kaaluda senise TsÜS § 80 lõikes 3 sätestatud kohustusliku ajakomponendi tõlgendamist ajatemplipäringu ajahetkena, millal isik saab lisaks tehingu ja e-allkirja andmete olemasolule tõendada, et tahteavaldus on tehtud. Samal ajal ei tohi unustada, et käibes kasutatakse ka madalama tasemega e-allkirju, mille puhul tahteavalduse tegemise ja tehingu tegemise aja sidumise nõuet pole või võiks pidada piisavaks e-allkirja andmise vahendi poolt määratud aega (sest madalama tasemega e-allkirjade puhul lisapäringuid usaldusteenuse osutajatele ei tehta). E-allkirja andmise aja fikseerimisest ei ole otstarbekas loobuda ka seetõttu, et tänu allkirjastamise täpsele ajale on võimalik allkirju masintöödelda. Automaatseks andmevahetuseks peavad infosüsteemid saama tugineda kokkulepitud ajaformaatidele.

Arvestades, et erinevalt TsÜS § 80 lõikest 3 ei nõua eIDAS-määrus e-allkirja sidumist tehingu tegemise ajaga, on küsitav, kas ka Eesti seadusandjal on kohane nii imperatiivsel kujul seda nõuda. Kui eIDAS-määruse jõustumisel 2016. aastal korraldati ümber seni digitaalallkirja seadusega reguleeritud e-allkirjade süsteem, võiks seadusandja kaaluda ka e-allkirjaga otseselt seotud tehingu elektroonilise vormi regulatsiooni ülevaatamist. Lisaks peab siinjuures silmas pidama, et kui juriidiline kohustus omakäelise allkirjaga

[42] RT I, 25.10.2016, 1; 12.12.2018, 30.

võrdväärsete e-allkirjade piiriüleseks tunnustamiseks tuleneb eIDAS-määrusest, siis riigiti on e-allkirja loomise protsess üles ehitatud erinevalt. Erinev võib olla nii e-allkirja konteineri sisu kui ka e-allkirja tehnilise loomise protsess.[*43]

4. Praktilised probleemid omakäelise allkirjaga võrdväärse e-allkirja andmise aja tuvastamisel

4.1. Omakäelise allkirjaga võrdväärse e-allkirja andmise sertifikaadi peatamine ja selle mõju aja tuvastamisele

Kui isik on kaotanud oma e-allkirjastamist võimaldava isikut tõendava dokumendi, see on varastatud või isikul on kahtlus, et seda võidakse kuritarvitada, saab elektroonilise dokumendi sertifikaadid peatada. Sertifikaat on elektrooniline tõend, mis seob isiku ja digitaalallkirja ehtsuse tõendamiseks vajalikud andmed ning kinnitab selle isiku samasust. ID-kaardi kiibil on kaks sertifikaati: üks sertifikaat on mõeldud isiku tuvastamiseks ning teine allkirja andmiseks. mobiil-ID puhul sertifikaadid SIM-kaardil ei asetse, kuid samuti nagu ID-kaardiga on ka mobiil-ID-ga kaasas kaks sertifikaati.[*44]

eIDAS-määruse artikli 28 lõige 5 ja artikli 38 lõige 5 annavad liikmesriigile õiguse kehtestada riigisiseseid eeskirju eIDAS-määruse nõudeid arvestades. eIDAS-määruse põhjenduspunktis 53 on selgitatud, et kvalifitseeritud sertifikaatide peatamine on mitme liikmesriigi puhul usaldusteenuse osutajate seas kindlalt väljakujunenud praktika, mis erineb tühistamisest, kuna toob kaasa ainult sertifikaadi ajutise kehtetuse. EUTS säte sertifikaadi peatamise lubamise kohta on sarnane varem kehtinud digitaalallkirja seaduse[*45] §-ga 12. ITDS § 9^5 kohaselt võib dokumendi väljaandja (Politsei- ja Piirivalveamet ning Välisministeerium) isikut tõendavasse dokumenti kantud sertifikaadi peatada ning peatatud sertifikaadi kehtivuse taastada EUTS §-des 17 ja 18 sätestatud tingimustel. EUTS § 17 lõige 1 annab usaldusteenuse osutajale õiguse peatada usaldusteenuse sertifikaadi kehtivus, kui tekib kahtlus, et sertifikaati on kantud valeandmed või sertifikaadis sisalduvale avalikule võtmele vastavat privaatvõtit on võimalik kasutada sertifikaadi omaja nõusolekuta. EUTS seletuskirja kohaselt antakse usaldusteenuse osutajale diskretsioon sertifikaadi peatamiseks, kui tekib kahtlus, et sertifikaati on kantud ebaõiged andmed või sertifikaadis sisalduvale avalikule võtmele vastavat privaatvõtit on võimalik kasutada sertifikaadi omaniku nõusolekuta. Formaalne protseduur avalduse esitamise korral ei ole otstarbekas, sest sertifikaadid võib olla vaja suurema kahju ärahoidmiseks peatada (ID-kaart koos paroolidega on kadunud) ning seda peab olema võimalik teha näiteks telefonikõne alusel. Avalduse menetlemine on aga pikem ning aeganõudvam protseduur.[*46]

Õiguskindluse huvides on vaja, et sertifikaadi staatus (kehtiv, peatatud või kehtetu) oleks alati selge ning selleks toimubki sertifikaadi kehtivuskinnituse kontroll, mille tegemise aeg märgitakse ka e-allkirja konteinerisse. Usaldusteenuse osutajad peavad olema kohustatud märkima sertifikaadi peatamise korral täpse ajavahemiku, mille jooksul sertifikaat on peatatud.[*47] EUTS § 17 lõike 3 kohaselt peab usaldusteenuse osutaja pärast sertifikaadi kehtivuse peatamist viivitamata kandma andmed kehtivuse peatamise kohta enda peetavasse sertifikaatide andmebaasi ning pidama arvestust sertifikaadi kehtivuse peatamise aja, aluse ja taotleja ning peatatuse lõpetamise kohta. Järelikult, kui usaldusteenuse osutaja sertifikaatide kehtivuse peatab, tuleb igal juhul kindlaks määrata konkreetne ajavahemik, mille jooksul sertifikaadid peatatud on.[*48] Tehniliselt on võimalik küll e-allkirja moodustamist alustada ka siis, kui sertifikaat on peatatud, sest e-allkirja andmise vahendiga saab luua baasallkirja ja ühtlasi saab teostada ka ajatemplipäringu, kuid arvestades, et ajatemplipäringu ja sertifikaadi kehtivuskinnituse päringu ajavahe saab Eesti praktikas olla maksimaalselt 15 minutit, on ebatõenäoline, et ajatemplipäringu ajahetkel oli sertifikaat peatatud

43 Käesoleva artikli mahtu arvestades ei ole analüüsitud eri riikide e-allkirjade tehnilisi komponente ega riigisiseseid õigusakte allkirjastamise aja määramisel.

44 Loe lähemalt: Mis on sertifikaadid. Arvutivõrgus: https://www.id.ee/index.php?id=30228 (08.05.2020).

45 RT I 2000, 26, 150, RT I, 14.03.2014, 12 (kehtetu).

46 Seletuskiri e-identimise ja e-tehingute usaldusteenuste seaduse eelnõu juurde, 237 SE. Arvutivõrgus: https://m.riigikogu.ee/tegevus/eelnoud/eelnou/323afaca-cb96-4118-a675-2a2db388141e/ (08.05.2020).

47 eIDAS-määrus, põhjenduspunkt 53.

48 K. Laanest. L. Kask ID-kaardi turvariski õiguslikud probleemid. Tallinn 2017. Arvutivõrgus: https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/id-kaardi-turvarisk-oiguslikud-probleemid.pdf (08.05.2020).

staatusega ning kehtivuskinnituse päringu ajaks oli kehtivus taastatud. Peatatud sertifikaadiga kvalifitseeritud e-allkirja lõpuni ei looda.

Sertifikaadi peatatud oleku ning kehtivuse kontrolliks tehakse usaldusteenuse osutaja (Eestis nt SK ID Solutions AS) peetavasse sertifikaatide andmebaasi isiku sertifikaadi kehtivuskinnituse kontroll ehk kontrollitakse, kas konkreetsel ajahetkel sertifikaat, millega e-allkirjastatakse, kehtis, ning selle kohta lisatakse e-allkirja konteinerisse päringu tegemise kellaaeg. E-allkirja andmise sertifikaat peab kvalifitseeritud e-allkirja ehk omakäelise allkirjaga võrdväärse e-allkirja andmise ajal olema kehtiv. Seega ei ole peatatud sertifikaadiga võimalik e-allkirja anda ning EUTS § 17 lõike 5 järgi on sertifikaadi kehtivuse peatatuse ajal antud e-allkiri kehtetu. Üldjuhul on sertifikaadi peatamine pigem üksikjuhtum, kuid Eestis on toimunud ka ulatuslik sertifikaatide peatamine ID-kaardi kriisi ajal[*49], kui peatati 760 000 isiku ID-kaardi sertifikaadid.[*50] Peatamise lubatavus oli üks peamiseid põhjuseid, miks ID-kaardi kauguuendamine oli võimalik ning isikud ei pidanud füüsiliselt dokumente välja vahetama. Seega võimaldab sertifikaadi peatamine paindlikku lähenemist vahendi kasutamisele, kuna isikul (või riigil) on võimalik igasuguse kahtluse korral sertifikaat peatada ning sertifikaadi kehtivuse taastamise järel on isikul kohe võimalik ID-kaarti või mobiil-ID-d elektroonilistes teenustes kasutada ja e-allkirja anda. Kindlasti on see suurendanud kasutusmugavust. Sertifikaadi peatamine või kehtetuks tunnistamine ei mõjuta juba varem kehtiva sertifikaadiga antud e-allkirjade kehtivust, kui allkirjale on lisatud nõuetekohane ajatempel ja tehtud kehtivuskinnituse päring.

4.2. Omakäelise allkirjaga võrdväärse e-allkirja aja kokkuleppeline tuvastamine

Praktikas võib tekkida probleeme olukordades, kus lepingu jõustumine või sõlmituks lugemine seostatakse e-allkirja andmise ajaga. VÕS § 11 lõike 2 järgi ei peeta lepingut sõlmituks enne, kui lepingule on antud ettenähtud vorm, kui lepingupoolte vahelise kokkuleppe või ühe poole taotluse tõttu tuleb leping sõlmida kindlas vormis. eIDAS-määruse artikli 25 kohaselt ei tunnistata e-allkirja õiguslikult kehtetuks ega kohtumenetluses tõendamiskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta nõuetele, mis esitatakse omakäelise allkirjaga võrdväärsele e-allkirjale ehk kvalifitseeritud e-allkirjale. Levinud praktika kohaselt ei väljendata aega tahteavalduses või lepingus, vaid kasutatakse fraasi „leping loetakse sõlmituks digitaalsel allkirjastamisel“ või „leping jõustub mõlema poole digitaalsel allkirjastamisel“ ning jääb pooltevahelise praktika kujundada, milline on allkirjastamise aeg. Seda toetab ka VÕS § 11 lõige 4, mille kohaselt loetakse kirjalik leping sõlmituks, kui lepingupooled on lepingudokumendi allkirjastanud või vahetanud kummagi lepingupoole poolt allkirjastatud lepingudokumendid või kirjad. Kui allkirjastamise aeg on defineerimata ning ka tehniliselt väljendub eri ajamärgendites, võib tekkida küsimus, kas leping on jõustunud ning millal peab asuma lepingut täitma. Kui üldjuhul on aja määramisel oluline kuupäev, siis võib olla ka ajakriitilisi kokkuleppeid, mille puhul võimaldab allkirjastamise aeg kindlaks teha, kas tehingupool võis olla viivituses või mitte. Siinkohal on oluline roll pooltevahelisel praktikal ning samuti kanalil, kuidas tahteavaldus või leping teisele poolele esitatakse. Üheks võimaluseks on tahteavalduses või lepingus siiski välja tuua aeg, mis hetkest pooled soovivad õiguslikke tagajärgede realiseerumist.[*51] Kuna ajatemplipäring ja kehtivuskinnituse päring tehakse vahetult pärast e-allkirja andmise seadmesse PIN2 sisestamist ning ajatemplipäringu ja sertifikaadi kehtivuskinnituse päringu vahe ei või olla enam kui 15 minutit, langeb üldjuhul kõigi kolme komponendi aeg ühte kuupäeva, mistõttu allkirja andmise kuupäeva üle vaidlusi enamasti ei esine. Kui vaidluse all oleva asjaolu puhul on olulised ka minutid, siis artikli autorite hinnangul on kõige mõistlikum tugineda ajatemplipäringu ajale, mis näitab tegelikku maailmaaega, et välja selgitada, milline oli ajahetk, kui isik oli väljendanud oma tahet, ning kas see oli seotud tahteväljenduse aluseks olevate asjaoludega.

49 Sertifikaatide peatamise ja peatatuse lõpetamise kohta lähemalt loe samast.

50 Lähemalt vt Eesti peatab ligi 760 000 ID-kaardi sertifikaadid 3. novembri õhtust. 02.11.2017. Arvutivõrgus: https://www.id.ee/index.php?id=38339 (08.05.2020).

51 T. Mets ja A. Paršovs on samuti jõudnud seisukohale, et õiguslikult olulised kuupäevad (aeg) võiks siiski välja tuua ka allkirjastatavas dokumendis, vt T. Mets, A. Paršovs (viide 41).

5. Kokkuvõte

Artikli eesmärgiks oli võrrelda allkirjastamist ja allkirjastamise aja kindlaksmääramist analoogmaailmas ja elektroonilises keskkonnas. Reeglina ei ole allkirjastamise aja kindlakstegemine õiguslike tagajärgede saabumise aspektist vajalik ning seda ei nõuta ka seaduses. Tsiviilõiguslikult ei ole oluline, millal dokument koostati ja kokkuleppe hilisem vormistamine dokumendina ei välista õiguslike tagajärgede saabumist. Kui kirjaliku vorminõude täitmiseks on vajalik omakäeline allkirjastamine ning allkiri võiks asetseda tehingudokumendi lõpus, et näidata ära tehingu sisu ja ulatus, ei ole omakäeline allkiri õiguslikult defineeritud ning allkirjastamise aeg on nõutav vaid seaduses sätestatud juhtudel. Seevastu elektroonilises keskkonnas on allkirjastamisele seatava nõudena vajalik ka allkirjastamise aja kindlaksmääramine. Sellele vaatamata ei ole allkirjastamise aeg defineeritud ning samamoodi nagu analoogmaailmas on isiku tegeliku tahte hindamiseks vaja hinnata ka isiku käitumist, tava ning varem poolte vahel välja kujunenud või kokku lepitud praktikat.

Euroopa elektroonilist allkirjastamist käsitlev eIDAS-määrus ei kohusta samuti allkirjastamise aega määrama. Samas ei ole allkirja andmise aja nõudmine TsÜS-s autorite hinnangul vastuolus eIDAS-määrusega, kuna eIDAS-määrusest saab lugeda välja ajakomponendi fikseerimise kaudse nõude. Selleks et hinnata, milline e-allkirja andmiseks vajalik toiming tuleks siduda tehingu tegemise ajaga, analüüsiti artiklis omakäelise allkirjaga võrdväärse e-allkirja loomise protsessi.

E-allkirja andmise toimingu sidumine tehingu tegemise ajaga TsÜS § 80 lõike 3 tähenduses on sisult määratlemata. Õiguskindluse ning tehingukäibe usaldusväärsuse seisukohast ei ole otstarbekas e-allkirja andmise aja fikseerimisest loobuda, kuid tuleks kaaluda kas seaduse muutmist või tõlgenduspraktika kujundamist selliselt, et TsÜS § 80 lõikes 3 sätestatud kohustusliku ajana saaks käsitada ajatemplipäringu ajahetke. Kuna eIDAS-määrus kohustab kindla tasemega e-allkirju piiriüleselt tunnustama, tuleb kindlasti arvestada ka piiriülese praktikaga.

Autoritest: Laura Kask on Tartu Ülikooli õigusteaduskonna doktorant. Ta on Tartu Ülikooli IT-õiguse programmi külalislektor ja OÜ Proud Engineers tegevjuht.
Kristiina Laanest on Riigi Infosüsteemi Ameti õigusosakonna juhataja.

Autorid tänavad käesoleva artikli valmimisse panustanud Riigi Infosüsteemi Ameti elektroonilise identiteedi osakonna eksperte.