TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Stefan Vingerfeld

Haldusleping plokiahela tehnoloogiat kasutavas nutilepingus ja selle vastavus halduslepingu vorminõuetele

Magistritöö

Juhendaja
Dr. iur. Mario Rosentau

Tartu
2023

SISUKORD

SISSEJUHATUS

Euroopa Liit (EL) võimaldab nii tööjõu kui ka teenuste vaba liikumist, mis tähendab ka õiguslike dokumentide ühest tunnustamist liikmesriikide vahel. Elektroonilised allkirjad, mis on loodud mõne EL liikmesriigi poolt, võivad tulla mõnelt Eestis resideeruvalt EL kodanikult, kes kasutab enda koduriigi lahendust elektrooniliseks allkirjastamiseks. Küll aga millist allkirja tüüpi tuleks kasutada ja kas elektrooniliseks allkirjaks on iga allkiri, on magistritöö põhiteemaks. Autor kasutab töös elektroonilise allkirja mõiste all ka väljendit „vormi atribuut“[1] ja eristab seda allkirjastamisest kui toimingust. Dokumentide allkirjastamist Euroopa Liidu üleselt reguleerib (EL) määrus e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (ingl *electronic IDentification, Authentication and trust Services*, edaspidi eIDAS). eIDAS võeti vastu 23. juulil 2014. aastal Euroopa Liidu Nõukogu ja Euroopa Parlamendi poolt.[2] eIDAS määruse preambula punkt 2 järgi määruse eesmärk on lihtsustada rahvusvahelist digiteenuste kasutamist, et kõikidele teenusepakkujatele ja avalikele asutustele kehtiksid ühesugused nõuded, toimimisalused ja põhimõtted.

eIDAS määruse tulek on kasvatanud identifitseerimist pakkuvate teenuste osutajate[3] huvi uute tehnoloogiate, nt hajussüsteem ja plokiahel, vastu. Tegemist ei ole täiesti uute tehnoloogiatega, sest nende erivormid on juba kasutuses (sh hajusarhitektuuri tehnoloogiat kasutatakse Eesti e-teenustes[4]). Ometi pakuvad plokiahela tehnoloogia lahendused jätkuvalt kõneainet selle sobivuse kohta kehtiva õigusega. Plokiahela tehnoloogia laialdasem kasutamine on endaga kaasa toonud automatiseeritud tehingud, milles kasutatakse nutilepingute (ingl s*mart contract*) nimetuse all tuntuks saanud lahendusi. Kõige tuntum nutilepingute kasutusala on krüptovarade ülekandmine ühest elektroonilisest rahakotist teise. Nutilepingud on plokiahelal tuginevad programmid, mis täidavad neile etteantud toiminguid automaatselt juhul, kui määratletud eeldused on täidetud. Üldjuhul kasutatakse neid kokkulepete täitmiseks automatiseeritult selliselt, et lepingu pooled saavad kohe olla kindlad saavutatavas tulemuses ilma vahendajateta või vähese ajakuluga.[5] Näiteks hiljutine Saksamaa koalitsioonileping lubab lihtsat terviklikult väljatöötatud plokiahela tehnoloogiat ja kinnitab oma pühendumust asjakohasele regulatiivsele

[1] Rosentau, M. Digitaalsed õigusvormid ja IT-lepingu kohustuslik vorm. (käsikiri autori valduses), lk 10 ja 18.
[2] 23. juuli 2014. aasta Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. – ELT L 257/73.
[3] Edaspidi kui ka mõistena „usaldusteenuse pakkuja”.
[4] Riigi Infosüsteemi Amet. Dokumendivahetuskiht DHX. Arvutivõrgus: https://www.ria.ee/et/riigi-infosusteem/dokumendivahetuskiht-dhx.html (29.03.2023).
[5] IBM. What are smart contracts on blockchain? Arvutivõrgus: https://www.ibm.com/topics/smart-contracts (25.04.2022).

raamistikule nii Euroopas kui ka rahvusvahelisel tasandil.[6] Euroopa parlament rõhutab vajadusele reguleerida Euroopa Liidus krüptovarasid, plokiahelatehnoloogiat ja nutilepinguid.[7] See tähendab, et iga liikmesriik peaks vastavalt oma siseriiklikule õigusele tegelema aktiivselt uute tehnoloogiate lahtimõtestamisega. Nutilepinguga tehingu tegemiseks on igal kasutajal oma virtuaalne rahakott, milles on isiku tuvastamiseks vajalikud era- ja avalikud võtmed. Need võtmed toimuvad autentimisena nii, et ühel kindlal kasutajal on volitused toimingu tegemiseks. Plokiahelal põhinevate nutilepingute puhul tekib küsimus, kas need lepingud on käsitletavad lepingutena Eesti seaduste mõistes ja kas krüptovõtmega tehingu kinnitamine on võrdsustatav Eestis kasutatava digiallkirjaga, kui tehingu vorm on seadusest tulenev? Sellele küsimusele vastamiseks on magistritöö fookuses avalikus sektoris kasutatav leping, kus lepingu vormidele on seadusest tulenevad kohustuslikud vorminõuded, sh allkirja kohustuslikkuse nõue. Autor lähtub analüüsi tegemisel peamiselt halduslepingu formaalse õiguspärase eeldustest. Eestis on õiguslikus mõttes hajussüsteemide kasutus halduses suures osas analüüsimata ning selle teemalist eestikeelset kirjandust on vähe. Plokiahela tehnoloogiat kasutava õigusakti formaalse õiguspärasuse küsimuse lahendamine aitab kaasa diskussioonile, mis puudutab plokiahela kasutust Euroopa Liidus üldisemalt ja meie siseriiklike regulatsioonide vastavust nende kasutamiseks.

Haldusmenetluse seaduse (edaspidi HMS) § 99 lg 3 järgi sõlmitakse halduslepingu kirjalikult. Praktikas on riigiga seotud toimingute puhul hoitud ranget poliitikat, et avalikus sektoris nõutakse omakäelise allkirjaga võrdväärset allkirja, mida tänapäeval võrdsustakse elektroonilise allkirjaga. Eestis levinud elektrooniliseks allkirja tüübiks on digitaalallkiri. Samas ei ole see kõikide toimingute puhul põhjendatud. Sealjuures elektrooniliste allkirjade mõistete kasutus ja nende tasemete tähtsus on haldusmenetluse näitel jätkuvalt segadust tekitav. Haldusõiguses tuleb halduslepingute puhul vastavalt juhtumile halduslepingu vormi täitmist hinnata tsiviilõiguslike lepingute jõustumiseks ettenähtud korras, arvestades HMS-ga kehtestatud erisusi (HMS § 105 lg 1). Lepinguõiguse sätetes on mitmeid tingimusi, mille alusel tuvastatakse tehingu vorm, seades erinevad eeldused lihtkirjaliku, kirjaliku ja elektroonilise lepingu vormi jaoks, mille käsitlemine aitab mõista ka haldusaktile kehtivaid nõudeid. Üldjuhul nõutakse avalikus sektoris täna omakäelise allkirjaga võrdväärset allkirja ehk digitaalkirjaga dokumente, kuid kindlasti ei ole see kõikide toimingute puhul põhjendatud. Elektroonilise

[6] Koalitionsvertrag zwischen CDU, CSU und SPD (coalition agreement, 14 March 2018), p. 70 et seq. Arvutivõrgus:https://www.bundesregierung.de/Content/DE/StatischeSeiten/Breg/koalitionsvertrag-inhaltsverzeichnis.html (21.04.2022).

[7] Tshibende, L.-D. M. Smart Contracts: Issues of Property and Secuirty Rights. – DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law – The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press 2020, lk 248.

lepingu vormi nõude täitmiseks võivad elektroonilised allkirjad vastata teatud usaldustasemele (nt kvalifitseeritud elektrooniline allkiri). Lepinguõiguses endas on jäetud hall ala selles osas, millised elektroonilise allkirja tüübid täidavad tsiviilseadustiku üldosa seaduse (edaspidi TsÜS) § 80 lg 3 sätestatud tingimused. Seaduses kasutatud elektroonilise allkirja mõiste puhul ei ole võimalik selgelt eristada, mida tähendavad paljud üldmõisted nagu „e-allkiri, e-tempel, e-teenused“ jne. Tõsi, tehnilised kirjeldused selgitavad, millised on elektrooniliste allkirjade erinevad tasemed. Samas elektroonilise allkirja osas ei ole haldusmenetluse seaduses eristatud e-allkirjade eritasemete õiguslikke mõjusid ja puudub selgus, millisel juhul saab kasutada nõrgema taseme allkirja ja millised nõuavad tugevama tasemega allkirja. Eelnevast tulenevalt on magistritöö põhieesmärgiks analüüsida plokiahela tehnoloogiat kasutava nutilepingu vastavust vorminõuetele halduslepingu näitel ja sealhulgas leida, millised on hajusraamatu tehnoloogial põhineva elektroonilise allkirja taseme kasutamise võimalused kehtiva haldusmenetluse seaduse alusel.

Magistritöö on jaotatud neljaks peatükiks. Esimeses selgitatakse hajusraamatutehnoloogiat[8], sellel põhineva plokiahela mõisteid, tehnoloogia kasutust ja tüüpe. Teema parema mõistmise huvides on mõistete selgitamine esimeses peatükis vajalik ning teema keerukuse tõttu ei ole võimalik kõiki mõisteid nende mahu tõttu selgitada sissejuhatuses. Hajusraamatutehnoloogia lahtimõtestamine on vajalik mõistmaks, kuidas see tehnoloogia toimib ja milliseid võimalusi see endaga kaasa toob. Samuti kirjeldab autor eIDAS määrusest tulenevaid allkirjastamise nõudeid ja selle mõju elektrooniliste allkirjade kasutamisele Eestis. Teises peatükis kirjeldab autor halduslepingut ja nutilepingut, selle sisu ja käsitlust lepinguna. Analüüsitakse tahteavalduste esitamist kui tehingu tuuma. Töö kolmas peatükk jätkab nutilepingul põhineva halduslepingu analüüsi, kuid seab tähelepanu alla lepingu vormi. Autor analüüsib halduslepingu vorminõudeid, lepinguõiguse alusel tehingu õiguslikke põhimõtteid ning nutilepingul põhineva halduslepingu vastavust kehtivale õigusele. Töö neljandas peatükis analüüsib autor nutilepingul põhineva halduslepingu allkirja nõudeid ja hindab elektrooniliste allkirjade tasemete erisusi. Peamine tähelepanu on haldusmenetluses kasutatavate õigusaktide allkirja vorminõuetel, tüüpidel ja klassifikatsioonidel. Eesmärk on välja selgitada, kas plokiahelal põhinev elektrooniline allkiri vastab halduslepingule seaduses sätestatud allkirja nõudele ja eIDAS määrusest tulenevatele klassifikatsioonidele.

[8] Hajusraamatutehnoloogiat saab kirjeldada kui andmestruktuuri, mis kajastab algoritmis sätestatud loogika kohaselt kodeeritud arvestusraamatu andmeid, mida saab vahetada ja millel võib olla õiguslik tähendus.

Eelnevast lähtuvalt on magistritöö eesmärkide saavutamiseks lähtutud järgmistest peamistest uurimisküsimustest:

1. Kas ja kuidas on plokiahela tehnoloogiate kasutamine võimalik halduslepingu kirjaliku vorminõude täitmiseks?
2. Millisele tasemele vastab nutilepinguga antav elektrooniline allkiri ja kas see täidab halduslepingule sätestatud allkirja nõuet?

Autor püstitab uurimistöö hüpoteesiks, et nutilepingutel põhinev haldusleping vastab lepinguõiguse põhimõtetele, aga haldusmenetluses allkirjastamist reguleerivate õigusnormide sõnastused on aegunud ja puudub selgus e-allkirjade kvalifitseerimistaseme õiguslikest tagajärgedest. Töö põhieesmärgi saavutamiseks kasutas ja kombineeris autor peamiselt analüütilist, võrdlevat ja süstemaatilist meetodit. Magistritöö on kirjutatud süsteemse teoreetilise uuringuna. Magistritöös kasutatakse nii eesti-, kui ka inglise keelset kirjandust, millest viimane moodustab suurema osa. Peamisteks allikateks on haldusmenetluse seadus, eIDAS määrus ja kaasaegne võõrkeelne kirjandus antud teemal. Töö teoreetilise osas kirjutamisel on kasutatud õiguskirjandust ja -teaduslikke artikleid ning EL institutsioonide ja asutuste töödokumente. Oluline käsitlus hajusraamatu tehnoloogia kasutuselevõtu õiguslikest probleemidest on Anne Veerpalu 2021. aasta doktoritöö „*Regulatory challenges to the use of distributed ledger technology: Analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence*“.[9] Doktoritöös tuvastati võimalikke eelarvamusi hajusraamatu tehnoloogia vastu kehtivas õigussüsteemis, kaardistati võimalikke lahendusi tehnoloogia neutraalse põhimõtte ja funktsionaalse samaväärsuse alampõhimõtte alusel. Käesoleva töö eesmärk on erinev, sest analüüsib lähemalt uute tehnoloogiate kasutamist haldusmenetluses kasutatava halduslepingu puhul. Magistritöö teema on aktuaalne, kuna Euroopa Liit on andnud liikmesriikidele tugeva signaali võtta riigisüsteemidesse kasutusele uusi tehnoloogiad, sh hajussüsteeme ja plokiahel. Samuti on ka autoril huvi selle vastu, kuidas tehnoloogiline areng mõjutab ja esitab väljakutseid kehtivate õigusnormide tõlgendamisele.

Märksõnad: hajussüsteemid, plokiahel, eIDAS, nutileping, haldusleping, elektrooniline allkiri, avalik õigus.

[9] Veerpalu, A. Regulatory challenges to the use of distributed ledger technology: analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence. – Doktoritöö. Juhendaja Martin Ebers, Anna-Maria Osul. Tartu: Tartu Ülikooli Kirjastuse trükikoda.

1. HAJUSSÜSTEEMID JA PLOKIAHELA TEHNOLOOGIA NING ELEKTROONILIST ALLKIRJA REGULEERIV EIDAS MÄÄRUS

1.1. Hajussüsteem ja plokiahela mõisted

Hajusraamatutehnoloogia (ingl *Distributed Ledger Technology* ehk DLT) on detsentraliseeritud, võrgus hajutatud ja keskse vahendajata jagatav andmekandmise süsteem. Seega võiks eesti keeles sobida ka mõiste „hajussüsteem". Hajussüsteem on pearaamat, millesse kantakse andmeid ja teavet. Pearaamat on omakorda grupeeritud plokkideks, mis on moodustatud detsentraliseeritud virtuaalse valuuta skeemi abil.[10] Hajussüsteem eristub traditsioonilisest tsentraliseeritud andmebaasist selle poolest, et selle pearaamatut ei halda ega kontrolli keskvõim ega muu asutus. Teised osalejad kinnitavad pearaamatusse tehtud kandeid ja seejärel sünkroniseeritakse uued andmed täiendustena.[11] Jaotatud pearaamat on digitaalne andmekandja informatsioonile või andmetele. Plokiahel on kõige populaarsem hajutatud pearaamatu tehnoloogia vorm, mis on pälvinud viimastel aastatel suurt tähelepanu. Plokiahel on tehingutel põhinev hajus andmebaas, mis on jagatud kõigi selle kasutajate vahel. Igal kasutajal on koopia kõige uuemast ahelast, millele on salvestatud kõik tehtud tehingud. Kolm põhitehnoloogiat, mis moodustavad plokiahela süsteemi, on hajussüsteemi raamat, krüptovõtmete[12] kasutamine ja võrdvõrgustik (ingl *peer-to-peer network*) – neid kõiki saab muuta vastavalt plokiahela kasutusele. Plokiahela tehnoloogia võrgustikud jagunevad avatud pearaamatuks (ingl *permissionless-based networks*) ja suletud pearaamatuks (ingl *permission-based networks*). Kõige tuntumad plokiahelale rajatud avatud pearaamatud on Bitcoin ja Ethereum. Suletud pearaamatud on võrgud, kus ainult teatud nõuetele vastavatel osapooltel on õigus osaleda valideerimises ja loa andmise protsessis.[13]

Virtuaalvääringute tegemiseks on rahakott (ingl *wallet*) kui programm hoiustamaks isiku virtuaalvääringuid. Rahakoti kasutamiseks antakse isikule privaatne ja avalik võti, mille abil on võimalik teha virtuaalvääringuga tehinguid.[14] Tegelikult neid saab nimetada kui ka kontodeks,

[10] European Central Bank (ECB). Virtual Currency Schemes – A Further Analysis. Veebruar 2015. Arvutivõrgus: www.ecb.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, lk 33.
[11] Bank for International Settlements,. Permissioned distributed ledgers and the governance of money. BIS Working Papers No 924, Jaanuar 2021, lk 2.
[12] Eenmaa, H., Schmidt-Kessen, M. J. Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts. – Computer Law & Secuity Review, 2019/35, lk 7-10.
[13] Veerpalu, A. jt. The hybrid smart-contract agreement challenge to European electronic signature regulation". – International Journal of Law and Information Technology. Oxford University Press, 2020/28 (1), lk 9.
[14] Veerpalu, A. jt, lk 11-12.

mis on kasutaja valduses tehingute tegemiseks. Igal pearaamatu koopial on olemas andmed kõikidest ülekannetest, mis koosnevad krüpteeritud numbrite plokkide andmetest, mis on kokku ühendatud ja levitatavad tänu võrdvõrgustikule. Võrdvõrgustik moodustub juhtimis- või talitusvõimetelt samaväärsetest serveritest ehk võrgusõlmedest. Suur eelis võrdvõrgustikul on selle turvalisus. Nimelt ei ole võrdvõrgustikul keskset serverit, mida rünnates kogu võrk kokku kukuks. Andmekanded (transaktsioonid, mis võivad olla ka tehingud) seotakse krüpteeritud plokkide ja andmepakettidena katkematuks ahelaks, mida ei ole võimalik meelevaldselt, s.t ilma hajusraamatu sõlmede konsensuseta, muuta ega kustutada.[15] Hajustehnoloogia, mis tänu arvutikodeerimisele ja krüpteerimisele, on teinud võimalikuks hoida ja valideerida mitmeid koopiaid andmetest üle terve infotehnoloogia võrgustiku. Seega ei ole hajusraamatu kandeid võimalik kustutada, sest selle andmed ja versioonid on püsivalt süsteemis laiali hajutatud. Just turvalisus ja selle muutmatus on selle tehnoloogia puhul kõige silma paistvamad omadused.

Iga kanne või tehing, mis tehakse plokiahelas, kantakse plokki ja see kinnitatakse läbi sõlmede (ingl *node*). Samaaegselt saadetakse see kanne igasse sõlme, mis omakorda teeb selle täidetavuse automaatseks ja muutumatuks plokiahelas. Plokiahela süsteemis üksteisega ühendatud sõlmed jaotavad andmeid struktuuri vahel. See tagab selle, et igal sõlmel on pidevalt uuendatud koopia tehtud kannetest. Plokiahelas on määravaks lisaks hääletamisele ka kasutajate kaevandamisressursi jõukus. Töö tõendamise (ingl *Proof-of-work*) tehnika abil on tehingud kinnitatud ajaliselt ja kontrollitud terviku osana plokiahela registrist. Seda protsessi kutsutakse kaevandamiseks.[16] Plokiahela sõlmed ei ole aga tasuta. Panuse tõendamise (ingl *Proof of stake*) protokollides valitakse juhuslikult kinnitajad niivõrd suurele hulgale plokkidele, kui oli nende panuse suurus. Nende loomiseks on vaja kaevandajaid (ingl *miner*), kes kasutavad oma arvutiressurssi lahendamaks keerulisi krüptograafilisi tehteid kinnitamaks ja tõendamaks uusi kandeid plokiahelas. Kaevandajad saavad uue ploki loomise ja kinnitamise eest majanduslikku tulu krüptovaluutas (nt Bitcoin).[17] Seni ei ole veel teada, kuidas see süsteem jätkab toimimist kui kogu ettemääratud bitcoinide arv on algoritmiliselt ära jagatud.[18]

[15] Rosentau, M. Arvutivõrgu abil sõlmitud leping kui lepingu erivorm. – Juridica 10/2021, lk 700.
[16] Tai, E. T. T. Challenges of Smart Contracts. *Implementing* Excuses. – DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law – The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press 2020, lk 81.
[17] Eenmaa, H., Schmidt-Kessen, M. J. Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts. lk 8.
[18] Idelberger, F. Merging traditional contracts (or law) and (smart) e-contracts – a novel approach. Arvutivõrgus: https://lawgorithm.com.br/wp-content/uploads/2020/09/MLR2020-Florian-Idelberger.pdf (25.04.2022), lk 168-170.

Plokiahela tehnoloogiat saab ilmestada kõige rohkem just läbi avaliku pearaamatu kirjelduse. Avalik pearaamat salvestab kõiki tehinguid, mida kunagi on üldse tehtud ja selle koopia on jagatud igale kasutajale, kes on sellega ühendatud. Iga plokk on ühendatud järgmise plokiga, kasutades krüpteeritud allkirja. See võimaldab plokke ühendada nagu pearaamat, mida saab jagada ja kinnitada igaühega, kellel on vastav juurdepääs. Plokiahelal kannete kinnitamiseks ja tõendamiseks on vaja osalejate enda panust arvutiressursina. Kinnitamise mehhanism on disainitud selliselt, et pärast andmete üleslaadimist plokiahelasse ei ole seda võimalik enam muuta. Avaliku plokiahela kood tähendab seda, et tegemist on avatud allikaga ja plokiahela plokid on pidevas automatiseeritud muutumises.[19] Seega tegelikult ei mõjuta ühe subjekti poolt avaliku plokiahela kasutamine teiste kasutamist ja keegi ei saa takistada teisi seda kasutamast. Krüpteeritud kanded annavad tänu hajusraamatule võimaluse olla küllaltki avalik. Avaliku plokiahela puuduseks on see, et see mõjutab sellesse salvestamiseks sobivaid andmeid. See tähendab, et privaatseid või tundlikke andmeid ei tohiks plokiahelas salvestada. Seetõttu tuleb see teave kusagil mujal salvestada.[20]

Avalikku pearaamatut jagatakse arvutitega ühendatud võrgustikus või sõlmedes, mis on põhimõtteliselt nagu väikesed virtuaalserverid, ja on kättesaadavad kõikidele teistele süsteemis osalejatele.[21] Avaliku plokiahela negatiivne külg on privaatsuse puudumine ja selle detsentraliseeritus tähendab, et mitte keegi ei oma selle üle kontrolli ega vastutust, mistõttu selle valitsemine on keeruline. Plokiahelat on võimalik võltsida, kuid sellest jääb maha võltsimist tõendav märge. *Decentralized Autonomous Organization* ehk *DAO* juhtum avas diskussiooni plokiahelal põhinevate nutilepingute nõrkustest ja veakohtadest. *DAO* detsentraliseeritud investeerimisfondi tegevus ei jõudnud alatagi, sest keegi leidis selle süsteemis avalikuks tehtud lähtekoodist loogikavea, mis võimaldas tal enda kasuks pöörata ligi kolmandiku fondi varast.[22] Samas saab koostada privaatseid plokiahelaid vastavalt vajadusele, et selliseid juhtumeid vältida.

Plokiahel on endaga kaasa toonud automatiseeritud tehingud, milles kasutatakse nutilepingute nimetuse all tuntuks saanud lahendusi. Kõige tuntum nutilepingute kasutusala on krüptovarade

[19] de Caria R. Blockchain and Smart Contracts: Legal Issues and Regulatory Responses Between Public and Private Economic Law. – Corporate and Financial Markets Law, 2020 (1), lk 366.
[20] Law Commission. Smart legal contracts. Advice to Government. Presented to Parliament by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty. November 2021. Arvutivõrgus: https://www.lawcom.gov.uk/project/smart-contracts/ (10.04.2023), lk 10-11.
[21] DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law – The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press 2020.
[22] Tai, E. T. T. Formalizing contract law for smart contracts. – Tilburg Private Law Working Paper Series, 2017 (6), lk 3.

ülekandmine ühest rahakotist teise. Nutileping juurutati juba 90-ndatel Szabó poolt.[23] Szabó defineeris nutilepinguid kui nutiskripte, mis ei olnud veel algse visiooni järgi juriidilised lepinguid, kuid mis olid mõeldud just neid asendama. Szabó defineeris neid kui digitaalselt määratletud lubaduste kogumeid, mille raames täidavad protokollid lubadusi.[24] Nutileping on täielikult kodeeritud asendamaks poolte lepingu täitmise protsessi. Tegemist ei ole väga nutika lepinguga nagu nimi viitab ja mis suudaks iseseisvalt teha tarku otsuseid. Pigem saab selle all mõelda ise toimivat ja võimaluste rohket oskust.

Nutikas leping koosneb tarkvarast, mille mõte on vahendada digitaliseeritud objekte, kuid mis ei ole võrdsustatav kokkuleppena. Nutilepinguid nimetatakse osapooltevaheliste kohustuste allikaks, kuid need kohustused tulenevad juba eelnevalt väljakujunenud tahtest, mis on nutilepinguga vormistatud ja üle antud.[25] Õigusteadlane Mario Rosentau on kirjeldanud neid kui isesooritavaid aheltehinguid või lepingumonitore, mis teatavate tingimuste täitmisel või täitumisel sooritavad automaatselt ettenähtud (vastu)tehinguid või virtuaalseid toiminguid.[26] A. Veerpalu hinnangul võib mõelda, et kuna nutileping kasutab sama tehnoloogiat, mis kvalifitseerub elektroonilise tehnoloogia alla, siis on see lepingu vorm samaväärne paberil kirjutatud lepinguga.[27] Samale järeldusele on jõudnud Euroopa Liidu riikidest ka Itaalia, kes on reguleerinud nutilepingu mõistet ja selle kasutamist. Itaalia regulatsiooni järgi kui Itaalia asutuse poolt määratud suuniste alusel on tehingu pooled arvutipõhiselt tuvastatud, siis nutileping vastab kirjaliku lepingu nõuetele.[28] Plokiahelal olevat krüptovõtmete kasutamist on võimalik võrdsustada digitaalse allkirjaga. Teoorias peaks see täitma eelduse, et plokiahelale või sarnast tehnoloogiat kasutavale platvormile üleslaetud nutileping on võrreldav kirjaliku lepingu vormiga ka nõutava allkirja mõttes. Siiski allkirjast ainuüksi ei piisa ja nutileping peab jätkuvalt täitma ka teisi seadusest tulenevaid lepingu vormi tingimusi.

Plokiahela süsteemidel põhinevate andmesüsteemide rakendamine kehtivas õiguses on õigusteadlaste jaoks mahukas ja keeruline ülesanne, kuna tegemist on ülimalt uudse tehnoloogiaga. Sellest olenemata on oluline, et õigusteadus pidevalt jälgiks ja püüaks oma vaatest tõlgendada uusi tehnoloogiaid nagu plokiahel ja nutilepingud. Tehinguandmed on salvestatud plokkidena, mis on ahelana omavahel järjestikult seotud. Igas ploki ahelas on

[23] Tai, E. T. T. Formalizing contract law for smart contracts, lk 1.
[24] Woebbeking, M. K. The Impact of Smart Contracts on Traditional Concepts of Contract Law. – Journal of Intellectual Property, Information Technology and E-Commerce Law, 2019/10., lk 109.
[25] de Caria R. Blockchain and Smart Contracts: Legal Issues and Regulatory Responses Between Public and Private Economic Law, lk 367.
[26] Rosentau, M. Arvutivõrgu abil sõlmitud leping kui lepingu erivorm, lk 702.
[27] Veerpalu, A. jt., lk 6.
[28] Art 8-ter(2) DL 135/2018 of 14 December 2018, converted into law by Law 12/2019 of 11 February 2019.

eelmise ploki krüptograafiline räsi[29], mis võimaldab kontrollida plokkide järjekorda ja terviklikkust[30] Uue tehnoloogia potentsiaali katsetatakse juba mitmetes erinevates valdkondades. Näiteks Eesti on teine riik pärast Maltat, mis võttis 2022. a veebruari keskel Euroopa Liidu Intellektuaalomandi Ameti (EUIPO) loodud plokiahela lahenduse pilootprojekti korras kasutusele. Kaubamärgi ja disainiandmete keskse haldajana on EUIPO eesmärk vähendada info tsentraalse säilitamisega seotud ohte ja lihtsustada liikmete jaoks intellektuaalomandi teabe levitamist.[31] Plokiahela tehnoloogiat ei ole Eestis seadustega reguleeritud. Küll aga on osad riigid nagu Itaalia, Malta ning USA osariikidest Arizonas[32] ja Vermonti osariik, reguleerinud uusi innovaatilisi tehnoloogiaid.[33] Ameerika osariigid on tunnustanud plokiahelat ja nutilepinguid kui endaga õiguslikke tagajärgi kaasatoovateks. Arizona on vastu võtnud väga detailse regulatsiooni, millega on reguleeritud plokiahela ja nutilepingu mõiste.[34] Uue tehnoloogia reguleerimisega soovitakse luua selgust ja kindlust nende kasutajatele, et nad saaksid luusi uusi arendusi. Euroopa Komisjon on koostanud tegevuskava plokiahelatehnoloogiate kasutamisele võtmiseks. MiCA on keskne element suurest seadusandlikkust paketist, mille eesmärgiks on plokiahelatehnoloogiate raamistiku kehtestamine hiljemalt 2024 aastaks[35]. Väljapakutud strateegiate valguses näeb MiCA ette normistiku seoses emiteerimise või pakkumisega, kauplemise või krüptovaraga kauplemisega seotud teenuste osutamisel.[36]

Plokiahela tehnoloogia võime on hallata suurtes kogustes andmeid ja olla samal ajal võltsimiskindel. See on mõjutanud ettevõtlust sooviga eralduda vahendajatest nagu keskpangad, kohtud ja teised valitsusüksused. Plokiahel aitab tagada üksikisikute tegevuse koordineerimist ilma tehingute kehtivust tagava keskasutuseta.[37] Plokiahela kasutamise mõte

[29] Räsifunktsioon (inglese keeles *hash function*) on krüptograafias kasutatav ühesuunaline funktsioon tekstistringide kodeerimiseks.
[30] Veerpalu, A. jt., lk 9
[31] Registrite ja Infosüsteemide Keskus (RIK). RIK lõi ühenduse Euroopa Liidu kaubamärkide plokiahela võrguga. Arvutivõrgus: https://www.rik.ee/et/news/rik-loi-uhenduse-euroopa-liidu-kaubamarkide-plokiahela-vorguga (19.04.2023).
[32]Provision 44-7061 A, Arizona Bill HB 2417/2017. Arvutivõrgus: https://legiscan.com/AZ/text/HB2417/id/1497439, (19.04.2023). Provision 44-7061 A of the same bill.
[33] Veerpalu, A. jt., lk 13.
[34] de Caria R.Definitions of Smart Contracts. Between Law and Code. – DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law – The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press 2020, lk 24-25.
[35] Magistritöö kirjutamise jooksul tuli teave, et Euroopa Parlamendi võttis 20.04.2023. a vastu krüptovara-turgude regulatsiooni.
[36] European Parliamentary Research Service. Markets in crypto-assets (MiCA), november 2022. Arvutivõrgus: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI(2022)739221_EN.pdf (10.01.2023).
[37] Eenmaa, H., Schmidt-Kessen, M. J. Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts, lk 5.

on luua uusi demokraatlikumaid või osaluspõhiseid otsustamissüsteeme, detsentraliseeritud või autonoomseid organisatsioone, mis võivad tegutseda üle võrgu inimese sekkumiseta. Samuti isetäitvate digitaalsete tehingute (nutiepingute) kasutamine. Eeldatakse, et plokiahel muudab radikaalselt sotsiaalseid ja majanduslikke struktuure, eemaldades kasupüüdvad organisatsioonid või vahendajad. Sellel on palju eeliseid: see tagab suurema läbipaistvuse, suurendab turvalisust, parandab jälgitavust, aitab vähendada halduskulusid ja suurendab tõhusust. Lubades osapooltel oma tehingute kohta korrektset arvestust pidada, võimaldab see neil vabaneda tsentraliseeritud, suurtest, korrumpeerunud vahendajatest, kellel on oma eesmärgid ja huvid. Plokiahela tehnoloogia arutelud takerduvad peamiselt tehnoloogia mitte mõistmise taha. Mis omakorda raskendab uute tehnoloogiate kasutusvõimalust ja paneb kahtluse alla nende sobivuse õiguslikkus mõttes. Järeldada võib, et detsentraliseeritud süsteemid pakuvad huvitavaid lahendusi praegustele tsentraliseeritud süsteemidele, kuid süsteemi kasutamise osas peaks siiski olema tugev kontrollraamistik, takistamaks detsentraliseeritud süsteemi loojatel endale disainida eelisvõimalusi süsteemi puudutavate otsuste tegemiseks. Plokiahela tehnoloogiat kasutavate nutilepingute puhul on pooltevahelised kokkulepped reguleeritud omaenda hajussüsteemi reeglistiku kohaselt ja tunduvad täiesti sõltumatud neile kohalduvast õigusraamistikust. Nutilepingute ning nende aluseks olevate tehnoloogiate arendajad on püüdnud luua ka virtuaalseid kohtuid.[38] Digitaalses maailmas on loodud võrgustik, mis justkui toimib enamjaolt sõltumatult kehtivast õigusest. Küll aga tehingu poolte vaheliste vaidluste ilmnemisel pöördutakse õiguste kaitseks riigi kohtusüsteemi poole, mis tegutseb riiklike ja rahvusvaheliste õigusnormide alusel. Vaidluste lahendamine traditsiooniliste kohtusüsteemide kaudu toob esile probleemid sellest, kuidas lugeda ja tõlgendada arvutikoodis väljendatud digitaalseid kokkuleppeid ja kas neid üldse saab pidada lepinguteks.

1.2. e**IDAS määruse mõju liikmesriikidele ja selle puudused**

eIDAS on Euroopa Liidus kehtiv e-identimise ja e-tehingute määrus, mis võeti vastu 23. juulil 2014. aastal Euroopa Liidu Nõukogu ja Euroopa Parlamendi poolt.[39] 2016 aasta 1. juulist hakkas kehtima eIDAS määruse nõue usaldusteenuste (sh e-allkirjade) piiriüleseks tunnustamiseks ja määrus on liikmesriikidele otsekohalduv. eIDAS määrusega seatud nõuded

[38] Aouidef Y., A., Federico A., Bruno D. Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects. Frontiers in Blockchain, 2021. Arvutivõrgus: https://www.frontiersin.org/article/10.3389/fbloc.2021.564551 (24.04.2022).

[39] 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.

on kohustuslikud avalikule sektorile ja e-teenustele. eIDAS määruse mõte on elektroonilise identifitseerimise ja usaldusteenuste ühtsed standardid, et võimaldada elektroonilisi tehinguid ELis. Selleks on eIDAS-i eesmärk ühtlustada elektrooniliste allkirjade reguleerimist, et neid saaks piiriüleselt usaldada, võimaldamaks veebitehinguid ja realiseerimaks veebipõhiseid ärivõimalusi. Seetõttu on eIDAS regulatiivne tööriist, mis rakendab tehnoloogianeutraalsuse põhimõtet, võimaldades piiriüleste elektrooniliste tehingute kasutamist, mis sisuliselt loob eeldused elektrooniliste tehingute käsitlemiseks funktsionaalselt samaväärsena paberkandjal tehtavate tehingutega.[40] eIDAS määrusest saab välja lugeda, et see rõhub peamiselt privaatsusele ja e-allkirja andmise kontrollmehhanismide olemasolule. Kuigi üheks eesmärgiks on ka märgitud tehnoloogia neutraalsus ja piiri ülene ühtne allkirjastamissüsteem, siis ei ole seda suudetud tagada. Autor eristab töös allkirjastamist kui toimingut ja kasutab elektroonilise allkirja mõiste all ka väljendit „vormi atribuut“, mille otstarve on luua kindel seos allkirja andnud isiku ja tema allkirjastatud dokumendi vahel.

eIDAS määruse kohaselt tuleb eristada nii eID kui ka e-allkirja tasemeid. eIDAS määruse kohaselt on eID ehk autentimislahenduste tagatistasemed järgmised: madal (ingl *low*), märkimisväärne (ingl *substantial*) ja kõrge (ingl *high*). Autentimine on elektrooniline protsess, mis võimaldab füüsilise või juriidilise isiku e-identimist või elektrooniliste andmete päritolu ja terviklikkuse kinnitamist (eIDAS artikkel 3 p 5). Autentimislahenduste mõte on tagada kõigile ELi residentidele ligipääs avaliku sektori pakutavatele avalikele e-teenustele oma riigi residentidega võrdväärsetel tingimustel. Isikutuvastamine madala taseme juures toimub tõendite alusel, mille põhjal võib eeldada, et isik on see, kes ta väidab olevat. Märkimisväärse taseme juures peab lisaks eelneva taseme nõuetele olema isikul ka riiklikult tunnustatud isikut tõendav dokument või teeb isikutuvastuse riigi poolt määratud pädevust omav haldusorgan. Kõrge taseme autentimise puhul nõutakse isikutuvastamiseks foto või biomeetriliste andmetega riiklikult tunnustatud isikut tõendavat dokumenti, mille puhul dokumendi ja identiteedi ehtsust on kontrollitud.[41] Selleks, et teada kas liikmesriigis pakutav autentimisteenus vastab nõutavale tasemele, saab seda Eesti puhul kontrollida Riigi Infosüsteemi Ameti kodulehelt või Euroopas eID kasutajate kogukonna foorumist[42]. Usaldusväärsuse tasemed on reguleeritud Komisjoni rakendusmääruses (EL) 2015/1502, 8. september 2015, millega kehtestatakse e-identimise vahendite usaldusväärsuse tasemete minimaalsed tehnilised kirjeldused ja menetlused vastavalt

[40] Veerpalu A., lk 129.
[41] Riigi Infosüsteemi Amet. Usaldusteenused ja koostöö. Arvutivõrgus: https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/usaldusteenused-ja-koostoo (19.03.2023).
[42] Kirova, M. Overview of pre-notified and notified eID schemes under eIDAS. Arvutivõrgus: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS (19.03.2023).

Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 8 lõikele 3.[43]

eIDAS määruse järgi jaotuvad e-allkirja tasemed järgmiselt: a) kvalifitseeritud e-allkiri; b) täiustatud e-allkiri, mis on antud kvalifitseeritud sertifikaadiga; c) täiustatud e-allkiri ja d) muud e-allkirjad, mis ei vasta eIDAS määruse nõuetele.[44] Vastavalt eIDAS määruse artikli 25 lg 2 on kvalifitseeritud e-allkiri võrdväärne omakäelise allkirjaga. Täiendavalt on nõutud, et allkirja andja kasutab allkirja loomisel kvalifitseeritud e-allkirja andmise vahendit. Näiteks eIDAS määruse artikkel 30 järgi peab allkirja andmiseks kasutatav kiip olema sertifitseeritud. Viimase eeldusena peab see põhinema e-allkirja kvalifitseeritud sertifikaadil ehk peab vastama eIDAS määruse artiklis 28 toodud nõuetele. Kvalifitseeritud e-allkiri ehk QES (ingl *qualified electronic signature*) loetakse võrdseks omakäelise allkirjaga. See on täiustatud allkiri, mis põhineb kvalifitseeritud sertifikaatidel ja on antud kvalifitseeritud allkirjaandmise vahendiga. Kvalifitseeritud sertifikaat on kui garantii, et sertifikaadi väljastamisel tuvastati füüsilise isiku identiteet. Kvalifitseeritud allkirja andmise vahend on samuti kui garantii, et allkirja loomiseks kasutatavad andmed (privaatvõti) on kindlalt allkirjastaja ainukontrolli all.

Täiustatud e-allkiri kvalifitseeritud sertifikaatidega ehk AdES/QC (ingl *advanced electronic signature with qualified certificates*) on täiustatud e-allkiri, mis põhineb küll kvalifitseeritud sertifikaadel, kuid ei kasuta kvalifitseeritud allkirja andmise vahendit. See tähendab, et allkirjastamise andmed (privaatvõti) võivad olla paigaldatud näiteks kasutaja arvutisse. Samas võib võti olla ka kiipkaardil, kuid seda vahendit ja selle loomist/jagamist pole auditeeritud ega sertifitseeritud (puudub garantii). Omakäelise allkirjaga võrdväärne elektrooniline allkiri on seega elektrooniline allkiri, mis eIDAS määruse artikkel 26 järgi vastab täiustatud e-allkirja nõuetele järgmistel tingimustel.

Täiustatud e-allkiri ehk AdES (ingl *advanced electronic signatuure*) peab täitma vähemalt järgmised miinimumnõuded: allkiri on seotud ainuüksi allakirjutajaga; allkirja abil on võimalik tuvastada allakirjutaja isikut; allkiri on loodud allkirjastamiseks vajalike andmetega, mis on ainult allkirjastaja ainukontrolli all ja allkiri on seotud allkirjastatud andmetega selliselt, et hilisemad andmete muudatused on tuvastatud.[45] Seega tuleb mõista, et allkirja kehtivus ja

[43] Komisjoni rakendusmäärus (EL) 2015/1502. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32015R1502 (21.03.2023).
[44] Kask, L. E-Eestist e-Euroopasse: elektrooniline allkiri riigisiseses ja piiriüleses suhtluses. – Juridica 10/2017, lk 676.
[45] Riigi Infosüsteemi Amet. Usaldusteenused ja koostöö. Arvutivõrgus: https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/usaldusteenused-ja-koostoo (19.03.2023).

vastavus omakäelisele allkirjale sõltub arusaamisest tehnilistest terminoloogiatest. Allkirja tüüpide tuvastamiseks on loodud demo-portaal,[46] mis suudab tuvastada täiustatud e-allkirju ja nende vastavust eIDAS määruse nõuetele.

eIDAS määruse mõte on luua ühtne raamistik elektroonilisele allkirjastamisele EL-s, kuid määrus on jätnud igale liikmesriigile lahtiseks määratleda nõuded, mida nad aktsepteerivad identifitseerimise mõttes ja see tekitab erinevused riikide vahel. eIDAS määruse artikkel 6 lg 1 punkt c asjaomane avaliku sektori asutus kasutab kõnealusele internetipõhisele teenusele juurdepääsuks usaldusväärsuse taset, mis on täiustatud või kvalifitseeritud allkiri. eIDAS määrus näeb ette identiteedi kontrollimise korra, millega kehtestatakse täiustatud elektroonilise allkirja (AES) ja kvalifitseeritud elektroonilise allkirja (QES) ühtne standard, mida saab tunnustada kõigis liikmesriikides. eIDAS-iga ühilduvaid allkirju kasutatakse tõenäolisemalt loaga hajussüsteemides, kus kasutajad on tuvastatavad.[47]

eIDAS määrus kasutab elektroonilise vormi allkirjastamiseks nn avaliku võtme infrastruktuuri (ingl *public-key infrastructure*, edaspidi PKI) PKI mudelit. Paljud tänapäeval kasutatavad identifitseerimissüsteemid põhinevad PKI mudelil, mis on avaliku võtmega krüptimisel ja digitaalsetel sertifikaatidel põhinev tehnoloogia. Paljudel riikidel on oma lahendused, kuidas valitsuste ja muude teenustega digitaalselt suhelda. PKI mudel tugineb kontrollitud institutsioonide poolt väljastatud digitaalsetele sertifikaatidele ja krüptograafiliste võtmete kasutamisele. Avaliku võtme taristu sõltub just sertifitseeritud usaldusteenuse pakkujatest. PKI kasutab sertifikaadiasutuses välja antud digitaalset sertifikaati, mis seob identiteedi (näiteks isik või ettevõte) krüptograafilise võtmepaariga. Kui dokument allkirjastatakse digitaalselt allakirjutaja privaatvõtmega, seotakse dokumendi täpne sisu ja allakirjutanu identiteet ainulaadse digitaalse jäljendi abil.[48] Kontrollitud usaldusteenuse pakkujad võivad olla nii avalikud kui ka erateenuse pakkujad, kellele riiklik pädev asutus on andnud kvalifitseeritud staatuse ja kes on kantud nn usaldusnimekirjadesse, mida tuntakse usaldusnimekirjade sirvijana või Euroopa usaldusnimekirjana (ingl *European List of Trusted Lists* (LOTL)).[49]

[46] DSS Demonstration WebAPP. Arvutivõrgus: https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation 17.03.2023.
[47] Law Commission. Smart legal contracts, lk 65-66.
[48] Secure Sockets Layer (SSL). Arvutivõrgus: https://www.ssl.com/et/KKK/faq-digitaalallkirjad-ja-dokumentide-allkirjastamine/ (12.10.2022).
[49] Euroopa komisjoni usaldusnimikiri kvalifitseeritud usaldusteenuse pakkujatest. Arvutivõrgus: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home (19.04.2023).
.

eIDAS määruse artikkel 27 lg 1 järgi, kui liikmesriik nõuab avaliku sektori asutuse poolt või tema nimel osutatava internetipõhise teenuse kasutamiseks täiustatud e-allkirja, tunnustab see liikmesriik täiustatud e-allkirju, e-allkirja kvalifitseeritud sertifikaadil põhinevaid täiustatud e-allkirju ja kvalifitseeritud e-allkirju, mis on antud vähemalt lõikes 5 osutatud formaadis või rakendusaktides määratletud meetodeid kasutades. Sama artikkel lg 2 sätestab, et kui liikmesriik nõuab avaliku sektori asutuse poolt või tema nimel osutatava internetipõhise teenuse kasutamiseks kvalifitseeritud sertifikaadil põhinevat täiustatud e-allkirja, tunnustab see liikmesriik kvalifitseeritud sertifikaadil põhinevaid täiustatud e-allkirju ja kvalifitseeritud e-allkirju, mis on antud vähemalt lõikes 5 osutatud formaadis või rakendusaktides määratletud meetodeid kasutades. Seega tuleb esmalt tuvastada, mis allkirja tüüpi siseriiklik seadus nõuab avaliku sektori õigusaktidele ja seejärel tuleb hinnata, millises e-allkirja standardformaadis see atribuut peab olema. Standarditele mitte vastavate e-allkirjade puhul jääb nende menetlemise piiriülese võimekuse tagamine allkirja looja riigile.[50] Sama artikkel 27 lg 5 sätestab, et komisjon võtab kehtivaid tavasid, standardeid ja liidu õigusakte arvestades hiljemalt 18. septembriks 2015 vastu rakendusaktid, milles määratakse kindlaks täiustatud e-allkirjade standardformaadid või alternatiivsete formaatide kasutamise korral standardmeetodid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega. eIDAS määruse rakendamiseks on loodud ka rakendusaktid, mis on e-allkirju käsitlev rakendusakt 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[51]. See rakendusakt viitab standarditele, millele vastavaid e-allkirju peavad Euroopa Liidu liikmesriigid olema võimelised käsitlema. Rakendusaktides on määratletud tehnilised kirjeldused ja nõuded toimingule ja millises standardformaadis see atribuut peab olema.

Üks olulistest eIDAS määruse nõuetest seab kohustuse tagada kõigile ELi residentidele ligipääs avaliku sektori pakutavatele avalikele e-teenustele oma riigi residentidega võrdväärsetel tingimustel. See tähendab, et kui e-teenuse portaali sisselogimisel nõutakse oma kodanikult mõnda autentimislahendust, siis tuleb aktsepteerida ka teiste ELi liikmesriikide samaväärse tagatistasemega autentimislahendusi, millest liikmesriigid on ametlikult teavitanud. Praktikas tähendab see seda, et kui portaal aktsepteerib eri tagatistasemega lahendusi (näiteks

[50] Kask, L., Laanest, K. Elektroonilise allkirjastamise aja tuvastamine. – Juridica 4/2020, lk 294.
[51] Komisjoni rakendusotsus (EL) 2015/1506. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32015D1506 (19.03.2023).

paroolikaart, ID-kaart), siis peab aktsepteerima kõiki liikmesriikide lahendusi, mis on kõrgema tasemega kui see kõige madalam, mida portaal nõuab oma riigi residendilt. Seda eeldades, et vastava riigi lahendus on kirjeldatud liikmesriikide eID lahenduste nimistus. Autori hinnangul on probleem eIDAS määruse lahenduses peamiselt tingitud sellest, et need rakendused on seotud ja väljastatud keskasutusele. See lahenduse valik muudab kasutajat sõltuvaks kolmandatest osapooltest ja juhtimine on kolmandate isikute kätes, mitte kasutajate endi käes. eIDAS määrusest tuleneva kontrollipõhimõtte järgi peab võtmete üle jääma kontroll, seega võtmete asukohaks ei tohiks olla virtuaalne server ehk nö pilvele laadimine.

1.3. eIDAS määruse puudused hajussüsteemide kasutamisel ja selle võimalikud muutused

eIDAS määruse nõrkade külgede kõrvaldamiseks avaldas Euroopa Komisjon 2021. aasta juunis ettepaneku eIDASe määruse läbivaatamiseks. eIDAS määruse raamistiku puuduseks nähakse mh seda, et see ei hõlma nn elektrooniliste atribuutide, nagu arstitõendid, juhiload või kutsekvalifikatsioonid, pakkumist. eIDAS määrus ei tunnusta ka hajussüsteemidel antud allkirju, mis tõttu on kahtluse all eIDAS määruse eesmärgi saavutamine olla neutraalne tehnoloogiate osas. Lisaks ei võimalda see kasutajatel piirata isikuandmete jagamist selliselt, et see oleks ainult selle teenuse saamiseks hädavajalik.[52] eIDAS määruse praeguse kehtiva redaktsiooni puhul on fookuses tsentraliseeritud lahendused, aga sedagi kavatasetakse muuta uues eIDAS 2.0 verisoonis.

Hajussüsteemi krüptograafias kasutatavad võtmed väljastatakse (olenevalt kasutaja eelistustest) protokolli kaudu otse kasutajale ja erinevalt PKI mudelist pole ühtegi teist isikut või asutust, kes neid võtmeid või protokolle tsentraalselt juhiks. Hajusraamatutehnoloogia[53] põhiste elektrooniliste allkirjade usaldusväärsus ei sõltu usaldussertifikaatidest ega usaldusteenuse pakkuja väljastatud privaatvõtmetest just seepärast, et võtmed, mida kasutatakse hajusraamatutehnoloogiale tuginevas allkirjastamisprotsessis (olenevalt kasutaja eelistustest), väljastab protokoll automaatselt otse kasutajale. Seega, erinevalt PKI-mudelist puudub hajussüsteemi puhul vajadus usaldusväärse vahendaja või ametiasutuse järele, kes neid allkirjastamiseks vajalikke võtmeid keskselt väljastaks ja haldaks. See siiski ei tähenda, et kõikidele hajusraamatutehnoloogiat kasutavatele tarkade lepingute kasutajatele saaks

[52] Busch, C. eIDAS 2.0: Digital Identity Services in The Platfrom Economy. – CERRE Issue paper, 10/2022, lk 12.
[53] Eesti keeleses komisjoni ettepanekus on kasutatud mõistet “e-arvestusraamat”. Töös piirdub autor otsetõlkega.

kinnitada, et see protokoll on funktsionaalselt samaväärne eIDAS määruse elektroonilise allkirja protokolli ja usaldussüsteemiga. See muudatus DLT infrastruktuuris seab PKI mudelil põhineva olemasoleva regulatsiooni ootamatul viisil proovile, kuna tsentraliseeritud usaldussüsteem pole enam ainus võimalus. Kontrollitavat auditilogi on hea omada ja see võib aidata hajutatud allikatest pärineva teabe hajutatud kogumisel. Kuid sellel on üks puudus – vastutuse puudumine. Probleem oleks lahendatav, kui tegemist oleks kinnise plokiahelaga, mis on riigi poolt hallatav ja järgitav. Hästi tugevalt reguleeritud plokiahel annab riigile vastutuse, jälgitavuse ja võimaldab kõiki pooli identifitseerida. Samas sellisel juhul ei ole plokiahela kasutamine enam mõttekas ja piisab lihtsalt hajussüsteemi andmebaasi tehnoloogilisest kasutamisest. Detsentraliseeritud lahendused pakuksid tugevamat turvalisust ja koondaks paremini andmed kokku, et neid hallata. Kuid tulenevalt tehnoloogia uudsusest ja tundmatusest ning selle kasutamise võimalustest, on detsentraliseeritud lahenduse kasutuselevõtt oma keerukuse tõttu liiga riskantne. Õiguskirjandust lugedes on autorile jäänud mulje, et tsentraliseeritud lahendused on domineerivad osaliselt seetõttu, et teadmised sellistest lahendustest on hetkel laialdased ja eIDAS määruse jaoks võiks see huvi pakkuda näiteks allkirjastamislahenduste puhul.

Komisjoni ettepaneku kohaselt on eIDAS 2.0 määruses sätestatud, et liikmesriigid on kohustatud nii pakkuma Euroopa digiidentiteeditasku (ingl *European Digital Identity Wallet,* EDIW) nii füüsilistele kui ka juriidilistele isikutele.[54] EDIW on sisuliselt tarkvararakendus, mis võimaldab kodanikke ja elanikke riikliku digitaalse identiteedi alusel veebis ja võrguühenduseta tuvastada. Uus Euroopa digiidentiteeditasku (EDIW), mis tagab küberturvalisuse ja privaatsuse kõrge taseme, on kriitilise tähtsusega. Selle asemel, et kehtestada kõigile Euroopa kodanikele püsiv ja kordumatu identifikaator, tundub eelistatavam privaatsussõbralikum alternatiiv – identifikaator, mis on iga teenuse kohta kordumatu ja seega ei võimalda kasutajate jälgimist erinevates teenustes.[55] Näitena on Euroopa Komisjoni digiasjade volinik Margrethe Vestager öelnud: „Euroopa digitaalne identiteet võimaldab meil lihtsalt ja ilma lisatasuta tegutseda igas liikmesriigis nagu kodus, olenemata sellest, kas soovime üürida korterit või avada pangakonto väljaspool oma päritoluriiki.“[56] Sel eesmärgil on eIDASi määruse läbivaatamise ettepanekule lisatud soovitus, milles sätestatakse EDIW tehnilised

[54] Euroopa Komisjoni ettepanek millega muudetakse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (eIDAS), seletuskiri. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281, artikkel 6a ja artikkel 12b (1) (edaspidi Euroopa Komisjoni ettepanek).
[55] Busch, C., lk 12.
[56] Pollet, M. Blockchain might be the solution to the digital identity hurdle. – EURACTIV France. https://www.euractiv.com/section/digital/news/blockchain-might-be-the-solution-to-the-digital-identity-hurdle/ (21.11.2022).

nõuded määratleva tööriistakasti väljatöötamise protsess.[57] Lisaks eID-de salvestamisele peavad kasutajad saama oma digiidentiteeditaskusse lisada muid elektroonilisi atribuute ja mandaate, nagu ülikoolikraad, diplomid, õpilastunnistused või juhiload. Ehk ei välistatud, et lähiajal tunnustame isikut tõendava dokumendi all QR koodi vahendusel esitatud andmestikku, mida politsei kontrollib näiteks juhtimisõiguse kontrollimiseks. Selline muutus avab mitmeid uusi põnevaid arutelusid dokumendi mõiste ja uue elektroonilise dokumendi vormi osas. Eeldad võib, et plaanitav eIDAS 2.0 pakub meil võimalust muuta Eestis tuntud ID-kaart oma vormil ja funktsioonil täielikult digitaalseks. Lihtsustatud öeldes puuduks meil kodanikuna kohustus kaasas kanda isikuttõendavat dokumenti kui ID-kaarti füüsilisel kujul, vaid vajadusel peab isik võimaldama selle esitamist elektroonilisel kujul. Autori hinnangul peaks see teoorias lõpuks täitma eIDAS määruse eesmärgi tagada üle Euroopaline ühine allkirja võrgustik. Euroopa digiidentiteeditasku peaks asendama Eesti puhul ID-kaarti. Järelikult võib eeldada, et tulevikus on euroopa kodanikul võimalik teostada elektroonilist allkirjastamist mistahes liikmesriigi allkirjastamist teenust kasutades. See tähendab, et hispaania kodanik peaks saama kasutada allkirjastamisteenust DigiDoc4 või sarnast Eestis pakutavat teenust.

Uue eIDAS 2.0 üle otsustakse eeldatavasti 2023. a sügisel ja selle vastuvõtmise korral hakatakse seda rakendama 2024. aastal. eIDAS määruse läbivaatamise ettepanekuga laiendatakse uut digitaalse identiteedi raamistikku ka juriidilistele isikutele. See tähendab ka identiteedi põhist digiidentiteeditasku isikutuvastuse kasutamist ka juriidilistele isikutele.[58] Euroopa Komisjoni eesmärk on luua digitaalse identiteedi lahenduste jaoks uus regulatiivne raamistik (eIDAS 2.0), mis vastab uutele turunõuetele ja annab kodanikele suurema kontrolli oma isikuandmete üle. Lisaks püüab digitaalturgude seadus (DMA) takistada digitaalse identiteedi teenuste platvormi hõlmamise ja väravahoidmise strateegiaid ning hoida seda turgu avatuna.[59] Selleks annab eIDAS määrus liikmesriikidele võimaluse valida mitme valiku vahel. Esimese variandi puhul väljastab liikmesriik ise oma kodanikele ja ettevõtetele digiidentiteeditasku või tellib rahakotirakenduse väljatöötamise ühelt pakkujalt valitsuse mandaadi alusel. Teine võimalus on, et liikmesriik määrab kindlaks reguleeriva ja turvalisuse raamistiku ning lubab mitme erasektori digiidentiteeditasku väljatöötamist ja tunnustamist liikmesriigis. Nende kahe võimaluse hulgas näib innovatsiooni ja valikuvabaduse edendamiseks eelistatavam konkurents erinevate digiidentiteeditasku rakenduste vahel, millest igaüks vastab asjakohastele tehnilistele ja juriidilistele nõuetele. Selline lähenemisviis

[57] Busch, C., lk 13
[58] Euroopa Komisjoni ettepanek, artikkel 6a(1).
[59] Busch, C., lk 5, 12.

võimaldab kodanikel vabalt otsustada, millist taskut nad soovivad kasutada. Eelkõige võib see lähenemisviis viia valitsuse väljastatud eID-de viljaka kombinatsioonini erasektori uuendustega kasutajasõbralike identiteedilahenduste jaoks. Selline lähenemine nõuab tehnilist lahendust, mis võimaldab koostalitlusvõimet teiste platvormidega.[60]

eIDAS proovib liikuda täiustatud ja mugavate lahenduste poole, mis suudavad integreerida kasutaja erinevaid kontrollitavaid andmeid ja sertifikaate. Kasutajatele määratakse digitaalne keskkond, kus saab kaasas kanda ja jagada erinevaid mandaate ja atribuute, nagu näiteks siseriiklikud eID, kutsetunnistused, ühistranspordikaardid või teatud juhtudel isegi digitaalsed kontserdipiletid. Need on nn iseseisvad rakendusepõhised digiidentiteeditaskud, mida hallatakse kasutaja mobiilseadmes, need võimaldab turvalist ja lihtsat juurdepääsu erinevatele nii avalikele kui ka erateenustele, mis on tema täieliku kontrolli all.[61] Muudatusettepanekust on oluline märkida, et eIDAS määrus ei kehtestanud ühtlustatud Euroopa digitaalset identiteeti, vaid pigem on suunatud olemasolevate digitaalse identiteedi skeemide vastastikuse tunnustamise ja koostalitlusvõime tagamisele riiklikul tasandil. Kõige suuremat kõneainet pakub Komisjoni ettepaneku punkt 11, mis kehtestab usaldusteenuste raamistiku elektrooniliste pearaamatute ja kvalifitseeritud elektrooniliste pearaamatute loomise ja hooldamise. See on oluline erinevate lahenduste puhul, mida saab ehitada hajusraamatutehnoloogiale ehk e-arvestusraamatud, sh kvalifitseeritud e-arvestusraamatud (ingl *electronic ledgers and qualified electronic ledgers*). Selgituse järgi plaanitakse kasutusele võtta elektroonilise pearaamatu mõiste kirjeldus, mis ühendab andmete ajatembeldamise ja nende järjestamise. Sellega tagatakse ka andmete õiguses nende koostaja suhtes nagu e-allkirjastamise puhul ning lisaeelisena võimaldab detsentraliseeritumat juhtimist. E-arvestusraamatutele õigusliku seisundi omistamine tähendab, et hajusraamatu (plokiahela) tehnoloogiale rajatud hajutatud usaldusteenused võrdsustatakse tsentraliseeritud, põhimõtteliselt riiklike, usaldusteenustega. Sellega langeb ära tehnoloogilise neutraalsuse põhimõtte rikkumine plokiahela tehnoloogiate suhtes, mida on eIDAS määrusele ette heidetud. Elektrooniliste pearaamatute üks suuremaid arusaamatusi on see, et neid nähakse kui tehnoloogilist lahendust, millel on konkreetne fikseeritud liigenergiat tarbiva tehnoloogia juurutamine. Komisjoni ettepaneku punktis 11 kirjeldatud elektroonilised pearaamatud kujutavad siiski endast tehniliselt neutraalset uue usaldusteenuse kirjeldust, mida iseloomustab elektrooniliste andmekirjete jada, mis tagab nende kronoloogilise järjestuse terviklikkuse ja täpsuse. Tänapäeval kasutavad paljud Euroopa uuendajad elektroonilisi pearaamatuid lahendustes, mis takistavad digitaalsete varade

[60] *Ibidem*, lk 16 ja Euroopa Komisjoni ettepanek, artikkel 6a.
[61] Komisjoni ettepanek, lõik 11 ja artikkel 45(h).

võltsimist, tõendavad või nõuavad ressursside omandiõigust, jälgivad tarneahelat ja digitaliseerivad intellektuaalomandi õigusi. Artikli 3 lõikes 53 ja jaotises 11 esitatud põhjalik sõnastus võimaldab kvalifitseerida paljusid elektrooniliste pearaamatute rakendamisi.

eIDAS määruse muudatus tooks kaasa detsentraliseeritud identifikaatorid (edaspidi DID), mis on uut tüüpi identifikaatorid kontrollitava, "iseseisva" digitaalse identiteedi jaoks. DID-id on täielikult DID-subjekti kontrolli all, sõltumata mistahes tsentraliseeritud registrist, identiteedi pakkujast või sertifitseerimisasutusest. DID juurutamiseks toetuvad iseseisva identiteedi kallal töötavad organisatsioonid identifikaatorite registri toetamiseks hajutatud pearaamatute kasutamisele. Eelkõige pakub detsentraliseeritud identiteedi sihtasutus (ingl *Decentralised Identity Foundation*) (DIF) tehnoloogilist arhitektuuri, mis põhineb järgmistel komponentidel. DID-dokument võib sisaldada vähemalt kolme asja: tõendamise eesmärgid, kontrollimeetodid ja teenuse lõpp-punktid.[62] Tõestuseesmärgid kombineeritakse kontrollimeetoditega, et luua mehhanismid atirbuutide tõestamiseks. Näiteks võib DID-dokument määrata, et autentimise eesmärgil loodud tõendi kontrollimiseks saab kasutada teatud kontrollimeetodit, nagu krüptograafiline avalik võti või pseudonüümne biomeetriline protokoll. Teenuse lõpp-punktid võimaldavad usaldusväärset suhtlust DID-kontrolleriga: DID-id on vaid anonüümneidentifikaator, ei anna nad teavet isiku enda kohta. Praktikas peaks DID-isid kasutama koos isikut tõendava teabega, mis muudab lihtsamaks digitaalse info vahendamise kolmandate osapooltega. Selliselt saab kolmandaatele isikutele tõendada, et DID-subjektil on teatud tõendite või atribuutide omandiõigus.[63]

Samamoodi laiendaks eIDAS 2.0 praegusi elektroonilisi usaldusteenuseid. Elektroonilised pearaamatud põhinevad nüüd DLT-tehnoloogial, pakkudes elektroonilisi arhiveerimisteenuseid ja hõlbustades kvalifitseeritud elektrooniliste allkirjade kaughaldust. Uue registri loomine suurendab ettevõtete suutlikkust kaitsta andmeid rikkumiste eest ning suurendab olemasolevate elektrooniliste tõendite hulka ja muudab need legitiimsemaks. Euroopa DIGITAL SME Alliance koos suuremate IT ja plokiahela lahendustega saatis Euroopa Parlamendi ITRE komisjoni liikmetele kirja, milles väljendab muret elektrooniliste pearaamatute, kui usaldusteenuste, eemaldamise üle elektrooniliste tehingute elektroonilise identifitseerimise ja usaldusteenuste hulgast. [64]

[62] Domingo, I. A. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market. – SSI eIDAS Legal Report. European Commission, 2020. eIDAS, lk 93-95.
[63] Decentralized Identifiers (DIDs). Arvutivõrgus: https://w3c.github.io/did-core/ (19.03.2023).
[64] Eurpean Digital SME Alliance. Digital SME pleads for blockchain as a security tool for EU Digital Identity. Arvutivõrgus: https://www.digitalsme.eu/digital-sme-pleads-for-blockchain-as-a-security-tool-for-eu-digital-identity/ (21.03.2023).

Magistritöö kirjutamisel ilmnes asjaolu, et ITRE komisjon võttis 9. veebruaril 2023 vastu eIDAS 2 ettepaneku uuema versiooni, mis ei sisalda enam 11. jaotist elektrooniliste pearaamatute kui reguleeritud usaldusteenuse kohta.[65] Euroopa Parlamendi viimane hääletus elektroonilise identifitseerimise määruse üle eemaldas plokiahela ja muud elektroonilised pearaamatud usaldusteenustena. Tegemist on üsna üllatava muudatusega ja jätab tähelepanuta, et elektrooniliste pearaamatute kontseptsioon on tegelikult tehnoloogiliselt neutraalne, kuna see kirjeldab pigem üldist kategooriat kui konkreetset rakendust. Selle kontseptsiooni määrusest eemaldamine võib tekitada palju probleeme, kus elektroonilisi pearaamatuid kasutatakse laialdaselt praegu usaldusarhitektuuri põhikomponendina. Elektroonilised pearaamatud on tõhusad küberrünnakute vastu ja need on olemas plokiahela ja hajutatud pearaamatu tehnoloogiates. Elektroonilisi pearaamatuid saab realiseerida erinevatel viisidel ja tehnoloogiatel nii tsentraliseeritud serveris kui ka detsentraliseeritud sõlmede võrgus. Eelnevast olenemata saab tulevase eIDAS 2.0 mõju kindlasti olema see, et edaspidi ei pruugi kõik allkirjastatud dokumendid olla tuntud DigiDoc4 Client programmiga loodud *DigiDoc signed* dokumendi tüübid, vaid mõnes muus vormis. See tekitab vajaduse kontrollida, kas dokumendile antud allkiri vastab ikka regulatsioonides nõutud allkirja nõudele. Elektroonilised pearaamatud erinevad suures osas elektroonilistest allkirjadest, pitserite või ajatemplite usaldusteenustest ja jääksid seega reguleerimata, kui need eIDAS 2.0 ettepanekust välja jäetaks.

[65] International Association for Trusted Blockchain Association internationale sans but lucratif. Open Letter for the preservation of the Electronic Ledger's provisions in eIDAS 2. 13. märts 2023. https://inatba.org/news/savesection11-eidas2-trusted-electronic-ledgers-open-letter/ (23.03.2023).

2. NUTILEPINGUT KASUTAVA HALDUSLEPINGU VASTAVUS KEHTIVALE ÕIGUSELE

2.1. Haldusleping ja selle vorminõuded

Haldusleping on kahe või enama vastastikuse tahteavalduse põhjal sõlmitud kokkulepe, mille sisuks on haldusõigussuhete tekkimine, muutumine või lõppemine.[66] Sarnaselt eraõiguslike õigussuhete reguleerimisele on ka haldusõigussuhete loomine, muutmine ning lõpetamine võimalik kahe või enama poole vahel kokkulepete alusel.[67] Halduslepingut reguleerib HMS-i 7. ptk. HMS § 95 järgi on haldusleping kokkulepe, mis reguleerib haldusõigussuhteid. Halduslepingu võib sõlmida kas üksikjuhtumi või piiritlemata arvu juhtumite reguleerimiseks. HMS § 96 järgi on vähemalt üks halduslepingu pool riik, kohaliku omavalitsuse üksus, muu avalik-õiguslik juriidiline isik, eraõiguslik juriidiline isik või füüsiline isik, kes seaduse alusel täidab avaliku halduse ülesandeid. Riigi või kohaliku omavalitsuse üksuse nimel sõlmib halduslepingu haldusorgan, kelle pädevuses on täita halduslepingu esemeks olev ülesanne. Haldusorgani pädevuses on avalike teenuste osutamise ülesanded, mida on teatud juhtudel otstarbekam sooritada kokkuleppe teel loodavate õigusaktide kaudu. Lihtsustatult öeldes kujutab haldusleping endast kahe või enama tahteavalduse põhjal sooritatud tehingut, millest üks lepingupool on haldusorgan ja mille sisuks on haldusõigussuhete tekkimine, lõppemine või muutmine. Lepingut peetakse halduslepinguks, kui sellega delegeeritakse eraisikule mingi haldusülesande täitmise kohustus ning delegeerimise tulemusel saab eraisik teatava voli kolmandate isikute üle, sealhulgas õiguse otsustada kolmandate isikute õiguste ja kohustuste üle.[68]

Haldusakti ning halduslepingu sisuline erinevus on minimaalne ning tavapärase haldusakti andmise asemel võib haldusorgan sõlmida halduslepingu, kui seadusest ei tulene teisiti.[69] Sama seisukohta kinnitab ka HMS § 98 lg 1, et haldusorgan võib haldusakti andmise asemel sõlmida üksikjuhtumi reguleerimiseks halduslepingu isikuga, kellele haldusakt oleks muidu suunatud, kui seadus või määrus ei näe otseselt ette üksnes haldusakti andmist. Valdav küsimus võib tekkida, et kui sisu poolest on haldusakt ja haldusleping sarnased, siis mille alusel sobivamat õigusakti valida. Esmalt tuleb tutvuda seaduse või määruse sõnastusega ja kui seaduse sõnastus

[66] Aedmaa, A., Lopman, E., Parrest, N., Pilving, I., Vene, E. Haldusmenetluse käsiraamat. Tallinn: Tartu Ülikooli Kirjastus 2004, lk 428.
[67] Aedmaa, A. jt, lk 427.
[68] Ginter, C., Parrest, N., Simovart M.A. Kontsessiooni vastuoluline regulatsioon Eesti õiguses. – Juridica IV/2012, lk 287-288.
[69] Aedmaa, A. jt, lk 431.

viitab üksnes õigusakti andmise võimalusele (nt korraldus või otsus), siis tuleks haldusakti vormi järgida. Kui aga õigusakti sõnastus on üldisem (nt "toetuse väljastab makseasutus") või seadus näeb alternatiivsete võimalustena ette nii haldusakti andmise kui ka halduslepingu sõlmimise, siis on mõeldav HMS § 98 lg 1 regulatsiooni rakendamine.[70] HMS § 97 lg 2 järgi haldusorgan võib sõlmida halduslepingu üksnes oma pädevuse piirides. Seega kui näiteks haldusorganile on määratud ülesandeks toetuste jagamine põllumajandustootjatele ja seaduses ei ole konkreetselt sõnastatud haldusakti andmist haldusorgani poolt, vaid nõutakse otsuse tegemist, võib haldusorgan seadustes määratud ülesannete täitmiseks sõlmida ka halduslepingu. Seaduses saavad toetuste väljaandmise tingimused lepingu osaks, mille täitmine on mõlemapoolne kohustus.

Halduskoostöö seadus (edaspidi HKTS) § 1 lg 1 järgi on seaduse mõte määrata kindlaks füüsilistele ja juriidilistele isikutele riigi ja kohaliku omavalitsuse avaliku halduse ülesannete (edaspidi *haldusülesannete*) iseseisvaks täitmiseks volitamise tingimused ja korra ning haldusorganite vahelise ametiabi osutamise alused ja korra. HKTS § 3 lg 4 teine lause näeb ette, et kui lepingust ei nähtu selgelt poolte tahe sõlmida tsiviilõiguslik leping, eeldatakse, et tegu on halduslepinguga. Seega avalike ülesannete täitmise tagamiseks sõlmitud leping kvalifitseerub halduslepinguks juhul, kui sellega on eraõiguslikule isikule antud avaliku võimu volitusi või kui leping reguleerib kolmandate isikute subjektiivseid avalikke õigusi. Kui aga halduslepingu sisuliselt vastab eraõiguslikule lepingule, siis seda käsitatakse tsiviilõigusliku lepinguna ja sellele kohalduvad lepinguõiguse tavalised normid. HKTS § 2 sätestab, et halduslepingule, mille ese on riigi ja kohaliku omavalitsuse haldusülesannete täitmiseks volitamine, kohaldatakse haldusmenetluse seadust, arvestades käesoleva seaduse erisusi. HTKS § 13 lg 1 järgi isikuga haldusülesande täitmiseks volitamise halduslepingu sõlmimisel juhindutakse riigihangete seaduses teenuste hankelepingu sõlmimise tingimustest ja riigihanke läbiviimise korrast.[71] Seega kui lepingu pooleks on isik, siis üldjuhul tuleb lepingu vorminõuete täitmiseks järgida riigihangete seaduses sätestatut. Küll aga HTKS § 13 lg 1^1 nimetab mitmeid olukordi, mille puhul halduslepingu sõlmimisel ei juhinduta riigihangete seadusest, nendeks on näiteks lepingud seoses tee-, raudtee-, vee- ja lennuliikluses ühistranspordi korraldamisega ühistranspordiseaduses või riigimetsa haldamine metsandusseadus. Nende lepingute puhul kohaldatakse haldusmenetluse seaduse sätteid.

[70] Aedmaa, A. jt, lk 433.
[71] Magistritöö piiratud mahu tõttu ei käsitle autor riigihangete seadusest tulenevaid formaalseid vorminõuded.

Haldusmenetluse läbivaks põhimõtteks on vormivabaduse printsiip (vt HMS § 5), mida seadusandja on oluliselt piiranud. Haldusaktid vormistatakse reeglina kirjalikult ning mingi muu vorm on võimalik erandina, kui seadus või määrus seda otsesõnu lubab, või kui on vaja anda edasilükkamatu korraldus.[72] Haldustegevuse ühepoolsus ei ole aga haldustegevust läbivalt iseloomustavaks jooneks – sarnaselt eraõiguslike õigussuhete reguleerimisele on ka haldusõigussuhete loomine, muutmine ning lõpetamine võimalik kahe või enama poole vaheliste kokkulepete alusel.[73] Halduslepingut võib kasutada olukordades, kus seaduses ei ole selgesõnaliselt sätestatud haldusakti kasutamist. Halduslepingul on haldusaktist oluliselt rangem vorm, sest viimast võib välja anda ka suuliselt. Halduslepingu kirjaliku vormi nõudel on samuti mitu funktsiooni. Esiteks tagab see hoiatusfunktsiooni, et lepingu sõlmimisel on teatud õiguslikud tagajärjed. Teiselt täidab see tõendamisfunktsiooni, et lepingu sõlmimine ja selle sisu oleks dokumentaalselt tõendatav.

Halduslepingu vormi kasutades jätab haldusorgan piltlikult öelduna kõrvale talle seadusega tagatud võimaluse teha ühepoolne, autoriteetne ning täitmisele kuuluv otsus, sõlmides selle asemel osapoolte kokkulepet ning konsensust eeldava, ent samas kohustava, ning täitmisele kuuluva halduslepingu. Halduslepinguga sõlmitav kokkulepe kujutab endast keskset mõistet eraõiguse sfääris ning sellele mõistele tugineb ka eraõiguslike õigussuhete üks mahukamaid alavaldkondi – lepinguõigus.[74] HMS § 101 lg 1 järgi üksikjuhtumit reguleeriv haldusleping jõustub tsiviilõiguslike lepingute jõustumiseks ettenähtud korras. Tehingu (lepingu) vormi seadusjärgsed nõuded on nii üldsätete kui ka analoogia korras rakendatavad pea kogu eraõigusest, samad nõuded on analoogia korras rakendatavad valdavas osas avalikust õigusest, ennekõike haldus- ja kohtumenetlustes. Halduslepingute liikide eristamisel tuleb järgida, et üksikjuhtumi reguleerimiseks antud haldusleping kujutab endast kokkuleppelisel viisil üksikakti andmist, piiritlemata arvu juhtumeid reguleeriv haldusleping aga kokkuleppelisel viisil üldakti andmist. Üksikjuhtumit reguleeriva halduslepingu korral on lepingust üheselt tuletatavad lepingu osapooled ning kolmandatele isikutele saab lepinguga täiendavaid kohustusi luua üksnes nende isikute nõusolekul. Piiritlemata arvu juhtumite reguleerimiseks sõlmitud halduslepingute korral ei ole lepingu pooled ja menetlusosalised kolmandad isikud (s.t isikud, kellele lepingust tulenevad konkreetsed õigused ja kohustused) üksikasjalikult määratletavad.[75]

[72] Aedmaa, A. jt, lk 294.
[73] *Ibidem*, lk 427-428.
[74] *Ibidem*, lk 427-429.
[75] *Ibidem*, lk 436.

Piiritlemata arvu juhtumeid käsitleva halduslepingu sõlmimisele on haldusmenetluse seaduses ette nähtud rida täiendavaid nõuded võrreldes tavalise, üksikjuhtumeid reguleeriva halduslepinguga. Nende nõuete kehtestamise vajalikkus tuleneb asjaolust, et enamasti ei ole piiritlemata arvu juhtumeid reguleerivate halduslepingute korral võimalik kaasata lepingu sõlmimise menetlusse kõiki isikuid, kelle õigusi ja kohustusi sõlmitav haldusleping võib puudutada. Seetõttu on õiguste riive oht piiritlemata arvu juhtumeid reguleerivate halduslepingute sõlmimise korral märkimisväärselt suurem kui üksikjuhtumit käsitlevate halduslepingute korral, kus lepinguga õigustatud ning kohustatud pooled on selgelt esile toodud. Alljärgnevalt on toodud loetelu piirangutest ning täiendavatest nõuetest, mis haldusmenetluse seadus piiritlemata arvu juhtumeid reguleerivate halduslepingute suhtes on kehtestanud:

- lepingu võib sõlmida üksnes seaduses sisalduva volitusnormi alusel (HMS § 97 lg 1);
- leping sõlmitakse kirjalikult tsiviilõiguslike lepingute sõlmimiseks ettenähtud korras (HMS § 99 lg 2);
- leping jõustub määruse jõustumiseks ettenähtud korras (HMS § 101 lg 4).

Piiritlemata arvu juhtumeid reguleeriv haldusleping eristub üksikjuhtumeid käsitlevast halduslepingust ennekõike kahe lisatingimuse poolest – seaduses sisalduv volitusnorm ning jõustumine analoogselt määruse jõustumisega. Mõlemad tunnused viitavad piiritlemata arvu juhtumeid reguleeriva halduslepingu olemuslikule seosele määrusega, kuna ka määruse puhul on selle andmise eelduseks seaduses sisalduva volitusnormi olemasolu (HMS § 90 lg 1) ning mõlemad õigusaktid jõustuvad kolmandal päeval pärast kehtivas korras avaldamist, kui õigusaktis endas ei ole sätestatud hilisemat tähtpäeva (HMS § 93 lg 2).[76] Kuna haldusülesande üleandmisel on avaldamise eesmärgiks teavitada kolmandaid isikuid uuest haldusorganist, siis halduslepingust teavitamata jätmine on aluseks lepingu tühisusele (HMS § 94 lg 2 p 1).

Oluline erinevus tsiviilõigusliku ja haldusõigusliku lepingu vahel on seotud lepingu kehtima hakkamise momendiga. Seega haldusleping peab olema kirjalikus vormis. Kirjaliku vorminõuete järgmiseks tuleb lepingu sisu ja selles seisnevat tehingut hinnata tsiviilõigusliku lepinguõiguse üldpõhimõtete ja normide alusel. Järelikult peab haldusleping sisaldama vähemalt kahte kattuvat tahteavaldust. Samuti ei ole lepinguõiguse reguleerivate normide all täpsustatud, millises allkirjastamise tüüp peaks olema antud sõlmitavale halduslepingule. Kuna

[76] *Ibidem*, lk 437.

HMS § 5 lg 1 annab võimaluse kasutada muud menetlustoimingu vormi, kui seadusest ei tulene teisiti, siis autor analüüsib järgnevalt halduslepingu kasutamist nutilepingu vormis.

2.2. Nutilepingu vastavus halduslepingu vormi reguleerivatele õigusnormidele

Lepingu vorm on oluline, sest teatud vara või õiguste võõrandamiseks võidakse riigisisese õiguse järgi nõuda kindlat kohustuslikku lepinguvormi. Nutilepingute vastavat kvalifitseerimist lepinguvormide tüpoloogia alusel on nimetatud oluliseks õigusküsimuseks ka Euroopa Liidu plokiahela uuringus.[77] Mario Rosentau on kirjeldanud neid kui isesooritavaid aheltehinguid või lepingumonitore, mis teatavate tingimuste täitmisel või täitumisel sooritavad automaatselt ettenähtud (vastu)tehinguid või virtuaalseid toiminguid.[78] Täpsem termin võiks olla kokkuleppeid täitev tarkvara, kuid arusaadavalt on nutileping kõnepruugis palju atraktiivsem. Ingliskeelses õiguskirjanduses on mõistete kasutamine kohati segadust tekitav, sest läbisegi kasutatakse nimetusi nagu nutileping (ingl *smart contract*)[79] ja algoritmiline leping (ingl *smart legal contract*) jättes tähelepanuta, et esimene neist ei pruugi sisaldada endas lepingut juriidilises mõttes. Õiguslikult on asjakohane rääkida nii nutilepingutest kui ka algoritmilistest lepingutest, pidades silmas, et nutilepinguid saab kasutada õiguslikke tagajärgi kaasa toovate kohustuste defineerimiseks ja nende täitmiseks, aga nende käsitlemine lepingutena igas olukorras oleks ennatlik.[80] Autor lähtub pigem üldsusele teada olevast nutilepingu mõistest. Nutilepingute oluliseks erisuseks on nende automatiseeritus. See tähendab, et osa või kõik lepingulised kohustused on täidetavad automaatselt ilma inimsekkumiseta. Ideaalis tähendab see seda, et programm ei ole võimeline keelduma või täitmata jätma lepingulist kohustust.[81] Seega kui lepingulised tingimused on saabunud, siis kokkulepitud kohustus täidetakse koheselt. Kuigi automatiseeritud tehingud on olnud kasutuses juba pikemat aega näiteks panga- ja kaardimaksete puhul, siis nutilepingute eripära seisneb võimaluses kirjutada see täielikult algoritmilise koodina ja viia täide hajussüsteemis. Plokiahel on väga sobiv platvorm nutilepinguteks, võimaldades veelgi suuremaid, paremaid, kiiremaid ja odavamaid tehinguid.[82]

---

[77] European Law Institute. ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection. – Report of the Euripean Law Institute, lk 24-27.
[78] Rosentau, M. Arvutivõrgu abil sõlmitud leping kui lepingu erivorm, lk 702.
[79] Nutileping juurutati juba 90-ndatel Szabó poolt. Szabó defineeris algoritmilisi lepinguid kui nutiskripte, mis ei olnud veel algse visiooni järgi veel juriidilised lepinguid, kuid mis olid mõeldud just neid asendama. Szabó defineeris neid kui digitaalselt määratletud lubaduste kogumit, mille raames täidavad protokollid lubadusi. Woebbeking, M. K, lk 109.
[80] Scholz, L. Algorithmic Contracts and Consumer Privacy. – Dimatteo L., Cannarsa M., Poncibo C. The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. – Cambridge University Press 2020, lk 255-257.
[81] Tai, E. T. T. Challenges of Smart Contracts. Implementing Excuses, lk 82-83.
[82] Eenmaa, H. Schmidt-Kessen, M. Regulation through code as a safeguard for implementing smart contracts in no-trust environments. – EUI Working Paper LAW, Itaalia, 2017/13, lk 11-12.

Y. Nguyên väidab, et nutileping ise ei ole veel juriidiliselt kasutatav – selleks oleks vaja kehtivat õiguslikku raamistikku.[83] Ta nimetab nutilepinguid arvutiprogrammideks, mis töötavad kahe või enama osapoole kokkulepitud parameetrite alusel. Arvutiprogrammi protokollid või koodid on mõeldud lepingu klauslite täitmise kontrollimiseks ja jõustamiseks, muutes seega mõned lepingu sõlmimise ja täitmisega seotud tegevused tarbetuks.[84] Haldusmenetluse seadus on üldosa seadus ja mõne eriseadusega võib ette näha halduslepingu sõlmimise ka muus vormis. Küll aga peab haldusleping olema vähemalt kirjalikus vormis, et täita tõendavat, hoiatavat ja selgitavat funktsiooni (HMS § 99 lg 3).[85] Eestis väljastatakse lisaks paberdokumendile ka elektroonilist dokumenti, mis lisaks isiku samasuse kontrollile digitaalses keskkonnas annab võimaluse elektrooniliselt oma tahte avaldust allkirja kaudu väljendada.

HMS § 100 järgi on haldusleping õiguspärane, kui ta vastab käesoleva seaduse §-des 54–57 või §-des 89–91 ja § 92 lõikes 2 sätestatud nõuetele. Nimetatud nõudeid kohaldatakse halduslepingule niivõrd, kuivõrd need ei ole vastuolus halduslepingu olemusega. Halduslepingu õiguspärasuse nõudest tulenevalt peab sõlmitav leping olema antud pädeva haldusorgani poolt. Halduslepingu vormilise õiguspärasuse kindlaks eelduseks on selle kirjalik vorm. HMS § 55 lg 2 kohaselt antakse haldusakt üldjuhul kirjalikus vormis, ent sellest reeglist on seaduse või määruse alusel võimalik teha erandeid, samuti võib haldusakti muus vormis anda edasilükkamatu korralduse tegemiseks. Halduslepingu saab seevastu sõlmida üksnes kirjalikus vormis (HMS § 99 lg 3). Haldusakti puhul on seadusega selgelt väljendatud, et kirjalikus vormis haldusakti võib anda elektrooniliselt (HMS § 55 lg 3). Kirjalik vorm on võrdsustatud elektroonilise vormiga, aga seaduse sõnastus ei anna selge vastust, kas ka iga elektroonilise vormiga. HMS-st endast ei tulene erandeid halduslepingu vormile, kui seda ei tee mõni eriseadus. HMS § 101 lg 1 järgi üksikjuhtumit reguleeriv haldusleping jõustub tsiviilõiguslike lepingute jõustumiseks ettenähtud korras. Üksikjuhtumi reguleerimiseks antava halduslepingu sõlmimise menetluse üksikasju HMS eraldi ei sätesta, selle asemel on viidatud üldisemalt haldusmenetluse seaduse esimesele osale (üldosa), mida kohaldatakse lepingu sõlmimisel niivõrd, kuivõrd see ei ole vastuolus halduslepingu olemusega. Lisaks kohalduvad halduslepingu sõlmimisele ka tsiviilõiguslike lepingute kohta käivad sätted, arvestades HMS-is kehtestatud erisusi (HMS § 105 lg 1).[86] Tsiviilõiguslike sätete kohaldamisest haldusõiguslikus suhtes on Riigikohus väljendanud end järgmiselt: „Avalik-õiguslikus suhtes

[83] Nguyên, Y. Artificial Intelligence Contract: How Algorithms and Machines have Disrupted the way Law is Practices. – PM World Journal, 2019/8 (9), lk 9.
[84] N Nguyên, Y, lk 10-11.
[85] A. Aeddmaa, jt., lk 440.
[86] *Ibidem*, lk 442.

võivad TsÜS normid olla kohaldatavad siis, kui neile on õigusaktides otse viidatud, või analoogia korras juhul, kui avalik-õiguslikke suhteid reguleerivates õigusaktides puuduvad asjakohased sätted.“[87] HMS ei sätesta selgelt halduslepingu vorminõudeid elektroonilisele vormile, mistõttu tuleb selleks kohaldada vastavaid lepinguõiguses kasutatavaid vormi sätteid.

Eriseaduseks HMS-i suhtes on ka halduskoostöö seadus (edaspidi HKTS), seetõttu tuleb haldusülesannete üleandmiseks lepingute sõlmimisel esmalt kohaldada HKTS-i ning alles siis HMS-i. Kui kohaldatavas seaduses on selge sõnaga sätestatud, et erasektori kaasamiseks avalike ülesannete täitmisel tuleb sõlmida haldusleping, ei teki küsimust, et kohaldamisele tuleb halduskoostöö seadus.[88] HKTS § 3 lõike 4 esimene lause sätestab, et haldusülesande täitmiseks volitamise korral võib sõlmida tsiviilõigusliku lepingu, kui seadus ei näe ette üksnes halduslepingu sõlmimist. Lepinguga ei reguleerita avaliku teenuse kasutaja või muu kolmanda isiku õigusi ega kohustusi, riiki või kohalikku omavalitsust ei vabastata tal lasuvatest kohustustest ja ülesande täitmisel ei kasutata täidesaatva riigivõimu volitusi. Seejuures näeb HKTS § 3 lõike 4 teine lause ette eelduse, et sõlmitud või sõlmitava lepingu puhul on tegemist halduslepinguga, kui lepingust ei nähtu selgelt poolte tahe sõlmida tsiviilõiguslik leping. Kui seadus lubab haldusülesannet üle anda, tuleb täita lisatingimused, näiteks tuleb koostada analüüs, mis peab tõendama, et haldusakti asemel halduslepingu sõlmimine on antud juhul tõepoolest mõistlik (majandusliku, õigusliku vms poole pealt) (HKTS § 5).

Halduslepingu peamine erinevus haldusaktist on see, et see annab võimaluse avalik-õiguslikke suhteid tekitada, luua ja lõpetada mitmepoolselt. Selle kasuteguriks on riigi muutmine isikupärasemaks, et selliselt oleks võimalik rohkem kaasata teist adressaati. Avalik-õigusliku ja eraõigusliku isiku vahelise lepingu sõlmimisel eeldatakse, et tegemist on halduslepinguga, kui lepingust selgelt ei nähtu poolte tahe sõlmida tsiviilõiguslik leping (HKTS § 3 lg 4 teine lause). Halduslepingut eraõiguslikest lepingutest eristab avaliku võimu volituste üleandmise asjaolu.[89] Seega halduslepinguga peab kaasnema see, et eraõiguslikule isikule on antud avaliku võimu volitusi või leping ise reguleerib kolmandate isikute subjektiivseid õigusi.

HMS § 35 lg 3 kohaselt algab haldusmenetlus halduslepingu sõlmimiseks vastava ettepaneku tegemisega. Kuna HMS ei kirjelda lähemalt halduslepingu kui kokkuleppe saavutamisega seonduvaid üksikasju, siis on siinkohal vajalik analoogia korras täiendavalt võlaõigusseaduse

[87] RKHKo nr 3-3-1-25-14 p 19
[88] Aedmaa A., Parrest, N. Haldusleping. Tallinn 2004, lk 28.
[89] *Ibidem*, lk 430.

kasutamine. Lepingu vormi klassifikatsioon on oluline tagamaks nende lepingute lugemine kehtivaks. Sellest tulenevalt on vaja leida vastus küsimusele, kas nutilepinguid saab kvalifitseerida elektroonilisel kujul lepinguteks, mis mõnes jurisdiktsioonis on samaväärsed kirjalike lepingutega.[90] Sellele küsimusele vastamiseks tuleb hinnata protsessi, kui nutileping või algoritmiline leping on sisestatud plokiahelale või hajussüsteemi platvormile nagu Ethereum. Sellisel juhul võib poolte tahte väljaselgitamisel vastavalt lepingu sisusele tõlgendada poolte tahet. Võlaõiguse seaduse (VÕS) § 9 lg 1 kohaselt sõlmitakse leping pakkumuse (oferdi) esitamise ning sellele nõustumuse (aktsepti) andmise teel.

2.2.1. Offert

Avaliku õiguse kontekstis on tahteavalduseks haldusorgani või haldusvälise isiku (menetlusosalise) poolt antud ning vahetult õiguslike tagajärgede loomisele suunatud avaldus.[91] Tahteavaldus väljendab kas avalduse tegija soovi tuua avaldusega kaasa õiguslikke tagajärgi (otsene tahteavaldus) või väljendub see teos, millest võib järeldada tahet tuua kaasa õiguslik tagajärg (kaudne tahteavaldus). Halduslepingu sõlmimisele kohalduvad ka tsiviilõiguslike lepingute kohta käivad sätted (HMS § 105 lg 1). Halduslepingu puhul on üheks oluliseks osaks tahteavaldus, mis annab pooltele tavaliselt rohkem menetluse käiku mõjutada. Eesti õiguskorras reguleerib tahteavaldust tsiviilseadustiku üldosa seadus. TsÜS § 67 lg 1 järgi loetakse tehinguks toimingut või omavahel seotud toimingute kogumit, milles sisaldub kindla õigusliku tagajärje kaasatoomisele suunatud tahteavaldus. Kui tehingu tegemiseks on vajalik kahe või enama isiku kahepoolne tahteavaldus, siis kujutab see endast mitmepoolset tehingut, mille sünonüümina kasutab TsÜS mõistet leping.

Halduslepingu puhul on poolte tahte väljaselgitamine olulise tähtsusega lepingu kvalifitseerimise osas. Lepingu tõlgendamisel on määrav poolte ühine tegelik tahe (VÕS § 29 lg 1). Riigikohtu praktika kohaselt kui lepingust ei nähtu poolte tahet sõlmida tsiviilõiguslik leping, tuleks see HKTS § 3 lg 4 teist lauset arvestades üldjuhul kvalifitseerida käsundilaadseks halduslepinguks.[92] Üldine põhimõte kohtupraktikas on see, et kui lepingust selgelt ei nähtu poolte tahe sõlmida tsiviilõiguslik leping, eeldatakse, et tegemist on halduslepinguga. [93] Juhul kui lepingust selgelt ei nähtu poolte tahe sõlmida tsiviilõiguslik leping, tuleb HKTS § 3 lg 4 järgi eeldada, et tegemist on halduslepinguga.

[90] Veerpalu, A., lk 129.
[91] Aedmaa, A., jt, lk 428.
[92] RKHKo nr 3-13-481, p-d 13-15.
[93] RKHKo nr 3-3-1-64-03, p 12, RKTKo nr 3-2-1-49-04, p 15.

Halduslepingu sõlmimise ettepanek kujutab endast seega pakkumust VÕS § 16 mõttes, ta peab olema kirjalikus vormis, piisavalt määratletud ning väljendama ettepaneku tegija tahet olla nõustumise korral sõlmitava lepinguga õiguslikult seotud. Sarnaselt pakkumusele peab ka nõustumine olema esitatud kirjalikus vormis. VÕS § 16 lg 1 mõttes on ofert lepingu sõlmimise ettepanek, mis on piisavalt määratletud ja väljendab oferendi (pakkumuse esitaja) tahet olla ettepaneku aktseptimise (nõustumuse andmise) korral sõlmitava lepinguga õiguslikult seotud. Ofert nõuab, et selles oleks väljendatud tahe olla lepinguliselt seotud isikuga, kes on aktsepteerinud tehtud pakkumise.[94] Lepingu sõlmimise ettepanekut, mille mittesiduvus on ettepaneku tegija poolt otse väljendatud või tuleneb lepingu olemusest, mille sõlmimiseks ettepanek tehti või muudest asjaoludest, loetakse ettepanekuks esitada pakkumus (VÕS § 16 lg 2). Reeglina loetakse ofert piisavalt määratletuks, kui selles sisalduvad lepingu olulised tingimused. Kuid ka lepingu oluliste tingimuste määratlemine ei anna alati võimalust üheselt määratleda, kas lepingu sõlmimise ettepanek on piisavalt määratletud või mitte. Lepingu sõlmimise ettepaneku hindamisel tuleb arvestada, kas ettepaneku tegija soovis teha oferdi või ainult ettepanekut oferdi tegemiseks.

Eraõiguse järgi TsÜS § 75 lg 1 alusel tuleb kindlale isikule tehtud tahteavaldust tõlgendada vastavalt tahteavalduse tegija tahtele, kui tahteavalduse saaja seda tahet teadis või pidi teadma. Kui tahteavalduse saaja tahteavalduse tegija tegelikku tahet ei teadnud ega pidanudki teadma, tuleb tahteavaldust tõlgendada nii, nagu tahteavalduse saajaga sarnane mõistlik isik seda samadel asjaoludel mõistma pidi. Kui tehingu tegemine väljendub mingis toimingus, mis sisaldab vastavat tahteavaldust, tuleb tehingut eristada nii sellistest toimingutest, mis ei too kaasa õiguslikke tagajärgi, st ei sisalda neile suunatud tahteavaldust, kui ka toimingutest, millega kaasnevad õiguslikud tagajärjed, kuid mis ei ole seejuures tehinguteks, näiteks teose avaldamine.[95] Lepingu sõlmimine eeldab üldjuhul pakkumist, vastuvõtmist, kaalumist ja vastastikust kavatsust end sellega siduda.

Oferti kui tahteavaldust saab tagasi võtta vastavasisulise tahteavaldusega, kui see jõuab oferdi adressaadini enne oferti või sellega ühel ajal (TsÜS § 72). Kuna nutilepingu puhul jõuavad tahteavaldused üksteiseni viivitamatult ja tehingud tehakse koheselt, siis ei ole alust rääkida tahteavalduste tagasivõtmisest enne, kui see teise lepingupooleni jõuab. Selle jaoks tuleb

[94] Varul, P., jt (koost). Võlaõigusseadus I. Üldosa (§§ 1 – 207). Komm. vlj. 2. tr. Tallinn: Juura 2016, p 4.1.1., lk 109.
[95] Varul, P., jt (2010). TsÜS § 75 komm. p 3.2., lk 218.

vaadata lähtekoodi ja selle protsessi, hindamaks seal avalduva tahte olemust. Võimalik on kaaluda ettepanekut VÕS § 16 lg 3 mõttes, kuivõrd tegemist on teenuse konkreetsele isikule mittesuunatud pakkumisega avalikus arvutivõrgus. Seda peamiselt seepärast, et ofert on suunatud kindlaks määramata isikute ringile. VÕS § 16 lg 1 kommentaaride järgi on leitud, et automaatmasinate puhul on tegemist pakkumisega teha pakkumus ning pakkumus on tehtud VÕS § 16 lg 3 mõttes siis, kui isik sisestab automaati raha.[96] Välja on pakutud ka, et hetk, mil mõlemad lepingu pooled on krüpteeritult lepingu allkirjastanud on lepingu pakkumise aktsepteerimise hetk, mitte aga hetk, kui tehing on kantud plokiahelasse.[97] Küll aga on pooled jõudnud ühisele kokkuleppele sündmustes, mis leiavad aset.

Sõltumata sellest, kas menetluse tulemusena lõpuks hallusleping sõlmitakse või mitte, loetakse haldusmenetlus pakkumuse esitamisega alanuks ning sellest momendist tekivad lepingu osalistel menetlusosalise õigused (õigus saada selgitusi, tutvuda dokumentidega, olla ära kuulatud jne). HMS § 43 lg 3 alusel halduslepingu sõlmimise menetlus lõpeb reeglina halduslepingu sõlmimisega, ent menetluse lõppemise alusena tulevad kõne alla veel ka kokkulepe halduslepingu sõlmimata jätmise kohta, ühe poole otsus jätta hallusleping sõlmimata ning halduslepingu poole surm või lõppemine. Sõlmitud hallusleping jõustub tsiviilõiguslike lepingute jõustumiseks ettenähtud korras (HMS § 101 lg 1) – hallusleping kui kirjalik leping loetakse sõlmituks, kui lepingupooled on lepingudokumendi allkirjastanud või vahetanud kummagi lepingupoole poolt allkirjastatud lepingudokumendid või kirjad (VÕS § 11 lg 4). Nutilepingute puhul ei lähtuta tahte tegija seesmisest tahtest, vaid sellest kuidas tahteavaldus on arusaadav mõistliku isiku vaatest (TsÜS § 75 lg 2 teine lause).

2.2.2. Aktsept

VÕS § 20 lg 1 järgi on nõustumus (ehk aktsept) otsese tahteavaldusega või mingi teoga väljendatud nõusolek sõlmida leping. Kui aktsept väljendub teos, mis ei ole otsene tahteavaldus, loetakse leping sõlmituks ajast, mil pakkumuse esitaja teost teada sai, välja arvatud siis, kui pakkumusest, lepingupoolte vahelisest praktikast või tavast tulenevalt loetakse leping sõlmituks alates teo tegemisest (VÕS § 9 lg 2, teine lause). Seega eristab võlaõigusseadus kahte võimalust lepingu sõlmituks lugemiseks, kui aktseptiks on tegu. Lepingu sõlmituks lugemiseks on oluline, et kokkuleppe saavutamine oleks piisavalt selge (VÕS § 9 lg 1).

[96] Varul, P., jt (2016). VÕS § 16 lg 3 p 4.3., lk 113.
[97] Veerpalu, A. jt., lk 18.

TsÜS § 75 lg 1 teise lause järgi tõlgendatakse tahet nii, kuidas oleks tahteavaldusest aru saanud tahteavalduse saajaga sarnane mõistlik isik samasugustel asjaoludel. Kokkuleppe saavutamine on piisavalt selge eelkõige siis, kui kokkulepe on saavutatud vähemalt lepingu olemuslikult olulistes tingimustes. Iga lepinguliigi puhul võib eristada tingimusi, mis määravad ära lepingu olemuse ja milles kokkuleppe saavutamisest võib järeldada poolte tahet olla lepinguliselt seotud. Niisugusteks tingimusteks on tavaliselt lepingu ese ja hind. Olenemata sellest lubab seadus osad lepingutingimused lahtiseks jätta, kui on selge, et lepingupooled soovivad olla lepinguga seotud. Nii ei too üldreeglina kokkuleppe puudumine ka hinnas kaasa lepingu mittesiduvust, kui ei saa eeldada poolte teistsugust tahet.

Digiajastul esineb selles õigusvormis enneolematul hulgal tahteavaldusi ja tehinguid. Samas, tehniliselt ei ole see vorm sugugi ühetaoline, vaid hõlmab väga erinevat tüüpi füüsilisi ja eriti digitaalseid esinemisvorme. Sestap on ehk just selle vormi kohta kõige rohkem külgi, mida uurida ja arutleda. Pakkumisena saab lugeda olukorda, et kus kasutaja vajutab „lae alla“ või „osta“ nupule või sisestab vastava rahasumma masinasse, mille järgselt toimub tehing automaatselt ilma täiendatavate läbirääkimisteta mõlemalt poolelt.[98] Sarnaselt sellele peetakse vaateaknal olevaid kaupu kutsena astuda tehingusse, samas kui müügiautomaadi klaasi taga olevaid tooteid peetakse kui pakkumisena, millele isik saab vastata nõustumisega kui sisestab raha müügiautomaati.[99] Sama põhimõtte kohaldub ka nutilepingutega tehtud tehingute puhul, kui *tokeni*[100] kuvamine süsteemis on vaadeldav müüja poolse pakkumisena, kui kutsena astuda tehingusse. Näiteks kui programm, mis on platvormil (nt Ethereum) teeb tehingu kandmaks selle *token* üle, kui selle eest on tasutud näiteks 5 krüptovääringuga. *Token* võib olla kui digitaalne vääringu väärtpaber, millele kohalduks väärtpaberituruseadus § 2 lg 1 p 1. Samamoodi pärast raha laekumist ei ole müüja ega ostja vahel läbirääkimisi.[101] Samuti on R. Brownsword seisukohal, et pakkumine ja nõustumine on nutilepingute puhul olemas.[102] Brownsword lähtus tingimusest, et nutilepingu sisu peab olema plokiahela kontekstis, et selle lepingu õiguse tingimused oleksid tehnoloogia poolt tagatud. Seega olenemata tehniliselt keerukusest on nutilepingud suutelised vahetama tahtavaldusi, mis toovad kaasa õiguslikke tagajärgi.

[98] Law Commission. Smart legal contracts, lk. 91-93.
[99] Gatteschi, V. Lamberti, F., Demartini C. Technologu of Smart Contracts. – DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law, lk 39 – 41.
[100] *Token* on plokiahela tehnoloogiat kasutav ja virtuaalväärингutega vahendav rahastamisviis.
[101] Law Commission. Smart legal contracts, lk 41.
[102] Brownsword, R. Regulatory Fitness: Fintech, Funny Money, and Smart Contracts. – European Business Organization Law Review, 2019, lk 15.

2.2.3. Kokkuleppe

Lepingu sõlmimisel lepitakse tavaliselt kokku lepingulistes kohustustes, kuidas neid tuleb täita ja millised tagajärjed on lepinguliste kohustuste rikkumisel või lõppemisel. Lepingu sõlmimiseni jõutakse tavaliselt siis, kui pooled on jõudnud kokkuleppeni lepingu tingimuste osas. Ka haldusleping on kahe või enama poole tahteavaldustele tuginev kokkulepe, mille esemeks on konkreetse haldusõigussuhte reguleerimine, täpsemalt mõne avaliku ülesande täitmine. Kui lepinguosalised pooled on omavahel lepingu tingimustes kokkuleppele jõudnud ning esitatud pakkumisele on vastatud nõustumusega, siis loetakse leping sõlmituks ning menetlus lõpetatuks. Sama kinnitab ka HMS § 43 lg 3, et halduslepingu sõlmimise menetlus lõpeb reeglina halduslepingu sõlmimisega, ent menetluse lõppemise alusena tulevad kõne alla veel ka kokkulepe halduslepingu sõlmimata jätmise kohta, ühe poole otsus jätta haldusleping sõlmimata ning halduslepingu poole surm või lõppemine. Sõlmitud haldusleping jõustub tsiviilõiguslike lepingute jõustumiseks ettenähtud korras (HMS § 101 lg 1) – haldusleping kui kirjalik leping loetakse sõlmituks, kui lepingupooled on lepingudokumendi allkirjastanud või vahetanud kummagi lepingupoole poolt allkirjastatud lepingudokumendid või kirjad (VÕS § 11 lg 4).[103]

Lepingutingimuste ebaselguse, mitmeti mõistetavuse või lünkade korral lepingus tuleb poolte tahte väljaselgitamiseks lepingut tõlgendada. Tahteavalduste tõlgendamisel tuleb lähtuda tsiviilseadustiku üldosas sätestatud tahteavalduste üldistest tõlgendamisreeglitest. TsÜS § 75 kohaselt arvestatakse tahteavalduse tõlgendamisel tahteavalduse tegija tahet, kui tahteavalduse saaja seda tahet teadis või pidi teadma. Kui tahteavalduse saaja ei teadnud, milline on tahteavalduse tegija tegelik tahe ega pidanudki seda teadma, siis hinnatakse tahteavaldust nii, nagu mõistlik isik seda samadel asjaoludel oleks sellest aru saanud. Ka avalikkusele tehtud tahteavalduse puhul on otsustavaks siiski see, kuidas oleks tahteavaldusest saanud aru mõistlik isik.[104]

Lepingu tõlgendamisel tuleb arvestada VÕS §-s 29 sätestatut. Lepingu kohaldamiseks tuleb seda tõlgendada ehk tuvastada, millise tähenduse andsid pooled tingimustele. Esmalt tuleb kindlaks teha poolte tegelik tahe subjektiivses mõttes. Kui seda ei ole võimalik kindlaks määrata, tuleb lähtuda objektiivsest tõlgendamisest. Sellisel juhul lähtutakse VÕS § 29 lg 4 mõttes, kuidas lepingupooltega sarnane mõistlik isik seda samadel asjaoludel pidi mõistma.

[103] A. Aedmaa jt, lk 443.
[104] Varul, P., jt (2010). TsÜS § 75 komm. p 3.1.1, lk 237.

Tõlgendamise esemeks võib olla kirjalik lepingudokument. Nutilepingu puhul tuleb ka võibolla hinnata arvutikoodis kirja pandut. Lepingutingimuste tõlgendamisel tuleb samuti arvestada tähendust, mida pooled ise andsid sellele tingimusele, mitte lähtuda üldlevinud tähendusest (VÕS § 29 lg 3). Tehingute tõlgendamise eesmärk muutub, kui tahteavaldusel on adressaat, kes ei tea ega pea teadma avaldaja tegelikku tahet. Sellisel juhul kasutatakse objektiivset tõlgendamist. Nutilepingute puhul ei pruugi üks lepingu pool kunagi teada saada teise poole tegelikku tahet, sest algoritm võib käituda vastavalt protsessile täitmaks oma eesmärki, mis ei ole veel vastavuses selle kasutaja lõpliku tahtega. Seega tuleks nutilepingute puhul esmalt lähtuda objektiivsest tõlgendamisest, sest avaldaja tegelikku tahte selgitamine on keeruline.

Lepingu poolte jaoks on oluline moment, millest alates loetakse leping sõlmituks, sest sellest momendist omandavad nad õiguslikult siduvad kohustused ning peavad sõlmitud lepingu täitma (VÕS § 8 lg 2). Vastavalt VÕS § 9 lg-le 2 loetakse oferdi aktseptimise korral leping sõlmituks alates ajast, mil oferdi teinud isik sai aktsepti kätte. Reeglina lepingu sõlmimisel lepivad pooled kokku et leping on sõlmitud kui pooled on selle allkirjastanud või viimane pool on selle allkirjastanud. Seega hakkab ka nutilepingu tüüpi kasutav haldusleping kehtima hetkest, kui leping on mõlemapoolselt allkirjastatud.

Seega kokkuvõttes nutilepingute korral saab tõlgendada pakkumist ja aktsepteerimist järgmiselt: pakkumine tehakse siis, kui masina omanik annab oma programmi sisestamisel süsteemile märku, et ta on valmis tehingu objekti vastu võtma. Aktsepteerimine toimub siis, kui klient annab oma tahte selles infosüsteemis. Ühepoolses lepingus, kus pool annab aga lubaduse midagi ette võtta, kui määratud toimingu sooritab keegi teine, piisab aktsepteerimiseks toimingu sooritamisest. Juhul kui tehingus saab olla rohkem kui kaks poolt, siis oleks selguse mõttes vaja täiendavaid tõendeid kinnitamaks kokkuleppele jõudmist. Näiteks võiks selleks olla üksikasjalik reeglistik, mis kirjeldab kokkuleppele jõudmise tingimusi. Pooled peavad aru saama oma tegevusest ja plokiahelast või platvormilt peab olema võimalik tuvastada õiguslikule tagajärjele suunatud tahteavalduse sisu. Tehingutes, mis on salvestatud jäädavalt plokiahelale ei olegi oluline otsese või kaudse tahteavalduse eristamine, kui tahteavaldus on infosüsteemis jäädavalt salvestatud.[105] Peaasi, et pooled saavad enda tegevusest aru ja salvestatud tahte tegemist on võimalik tuvastada ja tõendada õiguslikule tagajärjele suunatud tahteavalduse olemus ja sisu.[106] Selleks peab süsteemi üleslaetud arvutiprogramm olema loetav või vähemalt sobiv tõlgendamiseks inimesele loetavas keeles. Eeltoodust saab

[105] Varul, P. Tahteavaldus ja selle tegemine. – Juridica 2010/7, 497-500
[106] Rosentau, M. Arvutivõrgu abil sõlmitud leping kui lepingu erivorm, lk 698.

järeldada, et analoogmaailmas ja elektroonilises keskkonnas edastatud tahteavalduse tegemise ning kättesaamise õiguslikud nõuded ei erine. Elektrooniliselt edastatud tahteavalduse puhul loovad tehnilised vahendid paremad võimalused tahteavalduse kättesaamise kontrolliks. Mistõttu on ka nutilepingutega esitatud tahteavaldused õiguslikkus mõttes sobivad halduslepingu sõlmimiseks.

3. NUTILEPINGUT KASUTAVA HALDUSLEPINGU VASTAVUS LEPINGU VORMILE

3.1. Nutilepingute vastavus lepingu vormile

Lepingute puhul tuleb tähelepanu pöörata formaalsele vorminõudele. Selles osas tuleb hinnata, millised tehingu vormid ja erivormid võiksid kohalduda nutilepingutel. Üldpõhimõtte järgi on vorminõue täidetud, kui poolte arusaamine on selgelt väljendatud. Lepingu vorm peab olema nii hea, et sellest ei tekiks pooltele arusaamatusi lepingu tingimuste või väljendatud tahteavalduse osas. Kuigi nutilepingud võivad kujutada endast konkreetse lepingu tõlget, millel on juriidiline jõud kahe poole vahel, võivad need luua ka suhteid ilma lepinguliste õiguste ja kohustusteta.[107] Kehtivad seadused määratlevad, millistele vorminõuetele peab üks või teine õigussuhe vastama. Leping võib olla vabas vormis, kirjalikku taasesitamist võimaldavas vormis, elektroonilises vormis, notariaalselt kinnitatud (tõestamata leping) ja notariaalselt tõestatud leping. Täpsemalt vaatleb autor, mida kujutab endast elektroonilises vormis leping (nt e-allkirjaga leping).[108] Tehinguõiguses ette nähtud nõuded kohustuslikele vormidele tulenevad lepinguõigusest (täpsemalt VÕS-st). Lepingu vormi määramisel tuleb otsida teatud jälge või jälgida, mis lepingu sõlmimise toimingust maha jääb. Kirjaliku lepingu puhul on selleks peamiselt lepingudokument, mis on poolte poolt allkirjastatud. Halduslepingu kirjaliku vorminõue tuleneb juba avalikust asjaajamisest tuntud dokumenteerimiskohustusest.

Tsiviilseadustiku üldosa seaduse 4. peatükk reguleerib tehingu vormiga seonduvaid küsimusi. Vormivabaduse printsiibi sätestab Eesti õiguses TsÜS § 77 lõige 1, mille kohaselt võib tehingu teha mistahes vormis, kui seaduses ei ole sätestatud tehingu kohustuslikku vormi. Lepinguvabaduse põhimõte on põhiseadusest (PS § 19)[109] tuleneva enesemääramisõiguse ja privaatautonoomia väljenduseks ning tähendab seda, et võlasuhte tekkeks piisab reeglina ainult poolte kokkuleppest, ilma et sellele tuleks anda mingi kindel vorm.[110] See üldine tsiviilõiguses kehtiv põhimõte laieneb ka lepingutele ja tähendab lepingupoolte vabadust sõlmida leping suuliselt, kirjalikult või mistahes muus vormis, kui seaduses ei ole sätestatud lepingu kohustuslikku vormi (VÕS § 11 lg 1). Enamus võlaõigusseaduses reguleeritud lepingutest on üldjuhul vormivabad. Lepingut ei loeta

[107] Eenmaa, H., Schmidt-Kessen, M. J. Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts, lk 9.
[108] Rosentau M. Arvutivõrgu abil sõlmitud leping kui lepingu erivorm, lk 695.
[109] Madise, Ü. PSK § 26/2. – Eesti Vabariigi põhiseadus. Komm vlj. 5. vlj. Tallinn: Juura 2020, § 19 komm p 1-3.2.
[110] Varul, P., jt (2010). TsÜS § 77 lg 1, p 3.1., lk 244-245.

sõlmituks enne, kui lepingule on antud ettenähtud vorm (VÕS § 11 lg 2). Kehtivad seadused sätestavad vorminõude ranguse osas astmestiku, mille eesotsas on vabavorm (suuline, käitumuslik, nimetu jne), kirjalikku taasesitamist võimaldav vorm (nimeline allkirjata kirjatekst), (liht)kirjalik ja sellega võrdsustatud elektrooniline vorm (omakäelise või digiallkirjaga kirjatekst).[111] Kõige rangemad vormid on notariaalse kinnituse ja tõestuse vormid, mis oma olemuselt nõuavad eraldi uurimist.

Eraõiguses vormivabadus võimaldab pooltel kokku leppida näiteks, et nende omavahelises suhtes loetakse kirjaliku vormi nõue järgituks mitte ainult omakäeliselt allkirjastatud dokumendi, vaid ka faksi või e-kirja saatmise puhul.[112] Tehingu vorminõuded võivad tuleneda ka poolte kokkuleppest. Seda täiendab VÕS § 11 lg 1, mis lubab lepingu sõlmida suuliselt, kirjalikult või mis tahes vormis, kui seaduses ei ole sätestatud lepingu kohustuslikku vormi. Seega võivad tehingu pooled kokkuleppelise vorminõude korral ka vorminõuete sisu ise oma äranägemise järgi kujundada. Kui pooled on sõlminud lepingu mingis kindlas vormis, siis kehtib eeldus, et lepingudokumendis olev moodustabki kogu lepingu sisu. Siiski ei tähenda see, et lepingu sisuks ei võiks pidada ka muudest asjaoludest tulenevat (VÕS § 23 lg 1), välja arvatud juhul, kui lepingus on välistav tingimus, mis tuleneb VÕS §-st 31. Peamine küsimus on alati olnud, kas poolte vahel on kokkulepe ja milles pooled kokku leppisid. Kokkulepete kindlustamise mõttes on seadus pannud suurema väärtusega lepingutele vorminõuded, nagu kinnisvaratehingud peavad olema notariaalselt tõestatud.[113] Poolte kokkuleppest tuleneva vorminõude puhul tekib küsimus, kas näiteks kokkuleppelise kirjaliku vormi nõude järgimiseks peavad pooled täitma kõik TsÜS §-st 78 tulenevad kirjaliku vorminõude eeldused või võivad nad ka teisiti kokku leppida. TsÜS § 77 lg 2 järgi, kui nad seda ei ole teinud, kohaldatakse seaduses vastavale vormile sätestatud nõudeid. Lähtuvalt asja keerukusest ja riskist, võivad pooled kokku leppida, et nutilepingud peavad olema kirjalikud, vastamaks seaduse õiguslikule vormile. Sellisel juhul eeldatakse, et kehtivad selle vormi kohta seaduses sätestatud nõuded. Mistõttu on alust analüüsida, kas selline poolte vaheline võimalik ehk nutileping vastab kirjaliku lepingu vorminõuetele. Tõsi, vastavalt vormivabadusele saavad pooled põhimõtteliselt ise kokku leppida, mida nad loevad kirjalikuks vormiks. Näiteks loetaksegi kirjaliku vormi nõue täidetuks, kui see on nutilepingu vormis.

[111] Rosentau, M. Intellektuaalse omandi õigused infotehnoloogias IT autorilepingute kohustuslikud vormid ja vormiga fikseeritav sisu. – Juridica, 2020/5, lk 359.
[112] Sein, K. Lepingu vorminõuded ja nende järgimata jätmise tagajärjed. – Juridica 2010/7, lk 510.
[113] Idelberger, F. jt, lk 174.

Avalikus sektoris tuleb järgida seaduses sätestatut. HMS § 5 lõige 1 sätestab, et menetlustoimingu vormi ja muud haldusmenetluse üksikasjad määrab haldusorgan kaalutlusõiguse alusel, kui seaduse või määrusega ei ole sätestatud teisiti. Isik võib pöörduda haldusorgani poole peale kirjaliku vormi ka telefonitsi või mistahes muus vabalt valitud vormis. HMS § 5 lg 2 näeb ette, et haldusmenetlus viiakse läbi eesmärgipäraselt ja efektiivselt, samuti võimalikult lihtsalt ja kiirelt, vältides üleliigseid kulutusi ja ebameeldivusi isikutele. Kui seaduse või määrusega ei ole sätestatud teisiti, määrab menetlustoimingu vormi ja muud haldusmenetluse üksikasjad haldusorgan kaalutlusõiguse alusel (HMS § 5 lg 1) Ka HMS-s on elektrooniline asja ajamine võrdsustatud kirjaliku asjaajamisega ning lähtutakse EUTS-st (HMS § 5 lg 3).[114] Küll aga puudutab antud säte neid olukordi, kus halduslepingu kasutamist ei ole sõnasõnalt seaduses ette nähtud. Halduslepingu puhul on minimaalseks lepingu vormiks nõutav kirjalik vorm.

Näiteks võrdlusena on riigihangete seaduses (edaspidi RHS) lepingu vorm sätestatud §-s 8. Ka RHS § 8 puhul kehtivad hankelepingute suhtes eraõiguse üldnormid niivõrd, kuivõrd erinorm ei näe ette teisiti.[115] RHS § 8 lg 2 kolmanda lause alusel kohaldatakse hankelepingule VÕS-is ja teistes õigusaktides asjaomase lepinguliigi kohta sätesatud, kui RHS-is ei ole sätestatud teisiti. Järelikult hankeleping allub eraõiguse reeglistikule ka lepingu sõlmimise osas. Hankeleping on üldjuhul sõlmitud tüüptingimustel VÕS § 35 lg 1 tähenduses.[116] Tüüptingimused kuuluvad tõlgendamisele objektiivselt, st nii, nagu selles riigihankes osalev mõistlik ettevõtja tingimust samadel asjaoludel mõistma pidi (VÕS § 39 lg 1). Hankelepingu tõlgendamisel ei lähtuta poolte ühisest tahtest. RHS § 8 lg 7 reguleerib hankelepingu vormi. Normi esimene lause kehtestab hankelepingule kirjalikku taasesitamist võimaldava vormi nõude, kui hankelepingu maksumus on vähemalt 20 000 eurot. Eesti eraõiguslikud normid on riigihangete direktiivide omast rangemad.[117]

Võimalus oleks ka analüüsida nutilepingu plokiahelas kui püsivate andmekandjate vahetamisega sõlmitud lepingut (VÕS § 11^1). VÕS § 11^1 järgi püsiv andmekandja on vahend, mis võimaldab isikul säilitada isiklikult temale suunatud teavet nii, et see on teabe otstarbele vastava aja jooksul kättesaadav ja muutmata kujul taasesitatav. Püsiva andmekandja definitsiooni on vaja siis, kui seaduses on sätestatud teabe säilitamise vahendina püsiv

[114] Kask, L., lk 681.
[115] Simovart, M. A., Parind, Mart. Riigihangete seadus. Kommenteeritud väljaanne. Juura, Tallinn 2019, RHS § 8 lg 7, p 18, lk 99.
[116] RKTKo 2-15-15662/55, p 21.
[117] Simovart, M. A., Parind, Mart (2019) RHS § 8 komm, p 59, lk 111.

andmekandja. Püsivate andmekandjate liikideks on kõik kõvakettad jne. Täheldada tuleb, et püsiv andmekandja ja kirjalikku taasesitamist võimaldav vorm ei ole samatähenduslikud mõisted. Seaduse kommentaaride järgi on püsiv andmekandja, mis võimaldab isikul säilitada isiklikult temale suunatud teavet nii, et see on teabe otstarbele vastava aja jooksul kättesaadav ja muutmata kujul taasesitatav. Seadus eeldab, et teave oleks isikule adresseeritud selliselt, et oleks arusaadav, et see teave on mõeldud talle, teave peab olema muutmatul kujul taasesitatav ja olema muutmatult taasesitatav piisava aja jooksul, arvestades teabe sisu ja olulisust.[118] Küsitav on, kas plokiahelale kantud nutileping on püsiv andmekandja. Selleks tuleks hinnata digitaalsete andmekandjate sobivust, millest saab tuletada ka hajussüsteemil olevate lepingute võrdsustamist püsiva andmekandjaga. Küll aga kui andmekandjal ei sisaldu tahteavalduse tegija nime, siis puudub vajadus analüüsida seda vormi, kui eesmärk on leida nutilepingu võrdsus kirjaliku lepinguga. Samuti ei näe haldusmenetluse seadus halduslepingule otseselt ette võimalust sõlmida püsivate andmekandjate vahetamisega sõlmitud leping, mistõttu piirdutakse nutilepingu võrdlemisega seadusest ettenähtud lepingu vormidega.

3.1.1. Nutilepingu kui halduslepingu vastavus kirjalikku taasesitamist võimaldavale vormile

TsÜS § 78 lg 1 tulenevalt kui tehing peab olema tehtud kirjalikus vormis, siis peab tehingudokument olema tehingu teinud isikute poolt omakäeliselt allkirjastatud, kui seadusest ei tulene teisiti. Allkirjastamise nõude täidetavust käsitletakse süvitsi magistritöö 4.ndas peatükis. Kirjalikku taasesitamist võimaldavat vormi käsitletakse infotehnoloogia arengut ja infovahetust arvestava vormiga. TsÜS § 79 reguleerib kirjalikult taasesitamist võimaldavat vormi. Kirjaliku taasesitamise vormi mõte on teha tehing ja võimaldada sisu kättesaadavust tehingu ajal ja ka pärast tehingu tegemist, täites sellega nii tõendamis kui ka teavitamisfunktsiooni. TsÜS § 79 järgi kirjalikult taasesitatav vormi ei nõua erinevalt kirjalikust vormist omakäelist allkirja. Kirjalikku taasesitamist võimaldavas vormis tehtud tehingut peab olema võimalik taasesitada. Plokiahelale kantud lepingud on muutmatud. Mis tähendab, et plokiahelasse üles laetud lepingut, selle sisu ja arvutikoodi on võimalik lugeda kartmata, et see kunagi muutuks. Oluline ongi siin, et puudub teksti väljatrükkimise nõue, vaid seda teksti peab olema võimalik esitada loetaval viisil. Küll aga peab isikul olema võimalus mitte ainult seda lepingut lugeda, vaid ka ise salvestada ehk talletada enda tarbeks.

[118] Varul, P. jt (2016).VÕS § 11^1, p-d 4.2.-4.4, lk 78-79.

Selleks, et nutileping vastaks kirjalikult taasesitamist võimaldavale vormile TsÜS § 79 mõttes, peab nutilepingus olema esitatud tehingu teinud isikute nimed. Püsivat kirjalikku taasesitamist võimaldava viisiga ei tule arvatavasti probleemi, sest tehing on salvestatud digitaalselt plokiahelasse ja seda ei ole võimalik enam muuta. Mistõttu pärast lepingu sõlmimist ei ole leping enam poolte mõjusfääris, kes saaksid selle sisu hiljem muuta. Seega ka nutilepingu kodeeritud vormi nõudes võivad pooled kokku leppida ja kujundada oma tahte järgi. TsÜS-i kommentaaride järgi piisab ka pseudonüümist või hüüdnimest (ehk näiteks kasutajatunnusest), eeldusel, et see isik on teisele poolele selgelt identifitseeritav.[119] Selleks, et nutilepinguid saaks kasutada seaduse vormile vastavalt, tuleb nutilepinguid kasutada privaatses plokiahelas. Seal on plokiahela loojal võimalus määrata reeglid, mis võimaldab eelnevalt koguda andmeid, näiteks nime ja kõigi tehingu tegijate kohta. Neid andmeid saaks hiljem põhjendatud alusel nõuda tehingu tegijate identifitseerimiseks. Plokiahelale kantud lepingud on muutmatud. Mis tähendab, et plokiahelasse üles laetud lepingut, selle sisu ja arvutikoodi on võimalik lugeda kartmata, et see kunagi muutuks. Oluline ongi siin, et puudub teksti väljatrükkimise nõue, vaid seda teksti peab olema võimalik esitada loetaval viisil. Küll aga peab isikul olema võimalus mitte ainult seda lepingut lugeda, vaid ka ise salvestada ehk talletada seda ka endale.

3.1.2. Nutilepingu kui halduslepingu vastavus kirjaliku vormile

HMS § 99 lg 3 järgi halduslepingu sõlmitakse kirjalikult. Kirjaliku vorminõuded on täpsemalt sätestatud. Vastavalt VÕS § 11 lg-le 4 loetakse kirjalik leping sõlmituks, kui pooled on lepingudokumendid allkirjastanud või vahetanud allkirjastatud lepingudokumendid või kirjad. Nii tuleb TsÜS § 78 lg 1 kohaselt kirjaliku vorminõude korral tehingudokumentidele omakäeliselt alla kirjutada, kui seaduses ei ole sätestatud teisiti. Teatud juhtudel lubatakse ka allkirja mehaanilist jäljendamist (koopiana, trükitud allkiri). TsÜS § 78 lg 1 järgi on kirjaliku vorminõude põhinõudeks lepingu omakäeline allkirjastamine tehingut tegeva isiku poolt. Seaduse kommentaaride järgi kirjalik vorminõue ei eelda, et lepingus oleks märgitud tehingu tegemist koht ja aeg. Oluline on, et allkirja järgi saaks allkirjastatud isikut identifitseerida. Praktikas on tunnustatud ka allkirja mehaanilist jäljendamist. Seadus võib näha ette, et lepingulised tahteavaldused või teave tuleb esitada kirjalikku taasesitamist võimaldavas vormis. Sellisel juhul peab tehing sisaldama küll tehingu teinud isikute nimesid, kuid ei pea olema isiklikult allkirjastatud. Seaduse kommentaaride järgi piisab allakirjutanud isiku identifitseerimisest, kui lepingu allkirjas on kasutatud ainult perekonnanime ilma eesnimeta.[120]

[119] Varul, P., jt (2010). TsÜS § 79, p 3.3. lk 250.
[120] *Ibidem*, TsÜS § 78 komm. p 3.2., lk 247-248.

Järelikult, et nutileping vastaks kirjaliku lepingu vormile TsÜS § 78 mõttes, peab nutileping sisaldama kindlasti allkirja, mille järgi on võimalik isik identifitseerida. Tegemist ei pea olema omakäelise allkirjaga kui just teine pool seda ei nõua. Küll aga nutileping on elektrooniline, mistõttu ei sobitu see kirjaliku vormi (füüsilisel kujul, nt paberil) nõude alla TsÜS § 78 mõistes.

3.1.3. Nutilepingu kui halduslepingu vastavus elektroonilisele vormile

eIDAS määrus defineerib mõistet "elektroonilist dokumenti" kui igasugust elektroonilisel kujul salvestatud sisu, eelkõige teksti või heli, visuaalset või audiovisuaalset salvestist ja selle õiguslik mõju kehtib ka plokiahela "plokkidele". Seda toetab plokiahelapõhises registris või lepingus sisalduvate andmete juriidilist õigust. eIDAS määrus tunneb ära kolm erinevat e-allkirja taset: lihtne, täiustatud ja kvalifitseeritud. Plokiahelad näivad vastavat kahe esimese tehnilistele kriteeriumidele, kuid selleks, et olla õiguslikult siduvad, peavad need vastama kõrgeimatele standarditele. See nõuaks, et plokiahelatele antaks ka kõrgem kvalifitseering, mis võrdsustaks plokiahelal sõlmitud nutilepingu seaduse kehtestatud elektroonilise allkirjaga. [121] Seni pole seda Eestis tehtud, mistõttu kui seaduses kehtestatud lepinguvormile on ettemääratud allkirja nõue, siis plokiahelal olev allkirjastatud nutileping ei vasta seadusega sätestatud standardile. Eelnevast tulenevalt peavad eIDAS määruse alusel plokiahelas olevad digitaalallkirjad Euroopas juriidiliselt kehtima hakkamiseks olema kvalifitseeritud elektroonilised allkirjad. Kui nutileping neid eIDAS määruse nõudeid ei täida, ei saa nutilepingu tüübis sõlmitud lepingut kvalifitseerida elektrooniliseks, mis võib kehtiva regulatsiooni kohaselt osutuda takistuseks nutilepingute kasutamisel teatud tehingutes, mis nõuavad elektroonilist või käsitsi kirjutatud vormi.

TsÜS § 80 lg 1 järgi loetakse tehingu kirjaliku vormiga võrdseks tehingu elektrooniline vorm. Elektrooniline vorm tähendab, et leping on püsivat taasesitamist võimaldaval viisil vormistatud (TsÜS § 80 lg 2 p 1), sisaldab lepingu poolte nimesid (TsÜS § lg 2 p 2) ja on nende poolt elektrooniliselt allkirjastatud (TsÜS § 80 lg 2 p 3). Selleks, et elektrooniline vorm oleks võrdne kirjaliku vormiga peavad kõik nimetatud kolm tingimust täidetud olema. Lisaks peab ka elektrooniline allkiri vastama seaduses ettenähtud nõuetele, milleks on eelkõige võimalus seostada allkirja lepingu sisuga, lepingupoolte ja lepingu sõlmimise ajaga. TsÜS kommentaaride kohaselt on elektrooniline vorm võrdsustatud kirjaliku vormiga, kui elektroonilise vormi puhul on võimalik teha kindlaks tehingu tegija ja dokumendi ehtsus nagu

[121] Veerpalu, A. jt, lk 40.

kirjaliku vormi puhul.[122] Autor on seisukohal, et kuna plokiahelal olevate nutilepingute kasutajate krüptovõtmete kasutamise järgi ei saa viidata konkreetsele füüsilisele isikule (kas pseudonüümi või anonüümsuse tõttu), siis on keeruline tuvastada, kas sellel isikul ikkagi oli õigusvõime sõlmida leping. Ehk kui lepingupooled on täiesti anonüümsed, millelt meil saadeti, on autori hinnangul piisavalt meetmeid tuvastamaks e-maili kontot omavat isikut või vähemalt seadet. Olukorras, kus lepingupooled on täiesti anonüümsed ja hajussüsteemis endas on nõrgad poolte õiguskaitse meetmed, siis on meil tegemist traditsioonilisest õigusest teistsuguse usalduse (ingl *no-trust*) omadusega. Samuti on takistatud teatud seadusega kehtestatud vorminõuete täitmine, mis on praktikas jällegi vajalik. Vastasel juhul puudub pooltel õiguskindlus, kas nutileping vastav kirjalikule või elektroonilise vormi nõuetele õiguslikkus mõttes. Kartes keerukaid õigusvaidlusi ja tehingu tühisust, ei ole soodustatud nutilepingute kasutamine.

M. Rosentau hüpoteesi järgi seadusega sätestatud või poolte kokkuleppest tulenevalt kindlat tüüpi teabe esitamise kohustus kui selline, on osa seadusjärgsest või kokkuleppelisest vorminõudest. Seda on ta põhjendanud sellega, et teavitamiskohustus täidab kahte lepingule omast funktsioon. Selleks on poolte usaldusväärsus, kindluse tagamine ja hoiatusotsarve. Nimelt teine funktsioon peab täitma selle, et leping oleks väljendatud selgelt ja arusaadavalt. Ehk selle järgi kokkulepe peab sisaldama tingimusi määramaks lepingu sisu. See on oluline elektroonilise vormi puhul, kus digiallkirjad nõuavad lisaks sertifikaatidele ka andja nime andmeid (TsÜS § 80 lg 2 p 2). M. Rosentau peab seda seaduse lüngaks, mida peaks olema võimalik ületada analoogia kaudu elektroonilise vormiga. Samuti on ta leidnud, et just arvutivõrgus sõlmitavate lepingute tõttu on vajalik teabe esitamise kohustus, et tuvastada tehingu poolte tahteavaldused ja kokkuleppe sisu.[123] Jääb selgusetuks, millise lahenduse kaudu on mõeldud see lünk ületada. Autori hinnangul nutilepingute puhul ei ole teise tingimusega probleeme, sest kõik tehingud on salvestatud plokiahelasse või vähemalt võimalik tõendada nende ehtsust.

Samas puudub eIDAS-es nõue, et isikusamasuse seostamine allkirjaõigusliku isikuga peab olema allkirjastamistehnoloogia sisene võimekus ja et seda ei saa asendada lahendusega, mis suudab küll täita isikusamasuse tuvastamise funktsiooni, kuid on allkirjastamistehnoloogiast eraldiseisev. Alternatiivina kirjeldatud lahendusele võiks seadusandja kaaluda tehinguvormi ajutisi staatusi ehk tehinguvormi muutusi, kui allkirja seos isikuga on tekkinud. Anonüümsuse

[122]Varul, P., jt (2010). TsÜS § 80 komm, p 3.1., lk 251.
[123] Rosentau, M. Arvutivõrgu abil sõlmitud leping kui lepingu erivorm, lk 697.

tõttu oleks vaja täiendavaid meetmeid, mis aitaksid nutilepingu osas vaidluste ilmnemisel. Kuigi eIDAS määrus võimaldab ka allkirjastamist anonüümselt, siis avalikus sektoris sõlmitud lepingute puhul ei ole mõeldav, et haldusorgan sõlmib lepinguid anonüümsete isikutega.

Küll aga nagu eelnevalt on autor leidnud, siis plokiahelal kasutatav digitaalallkiri ei vasta seadusega kehtestatud standardile, mistõttu ei täida nutileping TsÜS § 80 lg 2 p 3 tingimust. Veel segasem on TsÜS § 80 lg 3 viimane lause, et elektrooniliseks allkirjaks on ka digitaalallkiri. Sätte sõnastusest võib justkui välja lugeda, et peale kvalifitseeritud elektroonilise allkirja on veel teisi elektroonilisi allkirju, mis võiksid vastata samale tasemele kui digitaalallkiri. Huvitav, kas seaduseandja üritas sellega edasi anda eIDAS määruse tehnoloogia neutraalsuse põhimõtet või pidas ta silmas ka muude elektrooniliste allkirjade kasutamist nagu nt hajussüsteemi põhinevat allkirja?[124] HMS endast ei tulene konkreetset nõuet, mis tüübis allkiri peab sõlmitud halduslepingul olema, mistõttu pööratakse sellele suuremat tähelepanu magistritöö järgmises peatükis.

Eelnevast tulenevalt saab asuda järeldusele, et nutilepingut on võimalik taasesitada, küll aga halduslepingule on seaduse ettenähtud vähemalt kirjalik vorm, mistõttu ei täidaks nutilepingut kasutav haldusleping seadusest tulenevat nõuet. Nutileping ei täida otseselt kirjaliku lepingu vormi, küll aga TsÜS § 80 lg 1 järgi on võrdsustatav kirjaliku vormiga kui leping kvalifitseerub ka elektroonilise vormi alla. Nutileping kvalifitseerub elektroonilise lepingu alla tingimusel, et sellele antud allkirja tüüp samaväärselt täidab elektroonilise allkirja tüüpi. Analüüsist tulenes, et nutilepingu vormis olev haldusleping vastab seadusest nõutavale elektroonilise lepingu vormile. Täitmaks ka allkirjastamise nõuet, tuleks nutilepingule lisada nii öelda väline allkirja tüüp, et see vastaks ka eIDAS määruse nõuetele ja seejuures täidaks seaduses nõutavat elektroonilise vormi tüüpi digitaalallkirja. Autor analüüsib allkirjadega seonduvat töö 4.ndas peatükis.

3.2. Halduslepingu vorminõude järgimata jätmise tagajärjed

Tehingute puhul tuleks ka alati rääkida olukordadest, mis tingivad tehingu tühisuse. HMS § 103 sätestab halduslepingu tühisuse tingimused. Haldusleping on tühine, kui tühine oleks sama sisuga haldusakt (HMS § 103 lg 1 p 1) või kui esinevad asjaolud, mis tingivad tsiviilõigusliku lepingu tühisuse (HMS § 103 lg 1 p 2). Olenemata sellest, kas tühisuse alused tulenesid

[124] Magistritöö kirjutamisel on aprillis 2023. aastal tulnud välja uus TsÜS kommenteeritud väljaanne, millest võibolla leidub vastuse autori küsimusele.

haldusõigusest või lepinguõiguse alustest, kohaldatakse tühisele halduslepingule tsiviilõiguslike lepingute tühisuse kohta sätestatut (HMS § 103 lg 2). Näiteks olukorras, kus haldusorgan tuvastab asjaolu pärast toetuse andmist, mille alusel toetust ei oleks antud, siis muutub haldusleping tühiseks. Tühisel lepingul puuduvad algusest peale õiguslikud tagajärjed, lepingu järgi saadu kuulub aga tagastamisele alusetu rikastumise sätete alusel. Halduslepingu muutmisel ning kehtetuks tunnistamine toimub tsiviilseadustes sätestatu alusel ja seega erinevalt haldusakti muutmisest ning lõpetamisest.

Haldusakti tühisuse alused sätestab HMS § 63 lg-s 2 välja toodud tingimused. Halduslepingu tühisuse aluseid on aga TsÜS erinevates sätetes. Tühiseks lepinguks on TsÜS sätete kohaselt näiteks esindusõiguseta isiku poolt sõlmitud leping (TsÜS 129 lg 1), näilik leping (TsÜS § 89 lg 2). Olukorras, kus pooled ei järgi seadusega kehtestatud vorminõuet, on poolte kokkuleppe tühine. TsÜS § 83 lg 1 järgi tehingu seaduses sätestatud vormi järgimata jätmise korral on tehing tühine, kui seadusest või vormi nõudmise eesmärgist ei tulene teisiti. Seega vastavalt tehingu sisule tuleb nutilepingu puhul jälgida, et see täidaks seadusest tulenevaid vorminõudeid. Vastasel korral on tehingu seadusest tuleneva vorminõude järgimata jätmise korral nutileping õiguslikus mõttes tühine. Juhul kui pooled on omavahel raamlepingus kokku leppinud, et kõik lepingud ja tehingud tuleb vormistada kirjalikult ja seadus ei kohusta tehingule kindlat vormi, siis tuleb järgida poolte kokkulepitust.

HMS § 102 lg 2 annab ühe konkreetselt halduslepingute suhtes kohalduva lõpetamise aluse, et haldusorgan võib halduslepingut ühepoolselt muuta või halduslepingu lõpetada, kui see on tingimata vajalik, et vältida ülekaaluka avaliku huvi rasket kahjustamist. Seejuures liigset ülemvõimu piirab sama paragrahvi lõige 4, et kui halduslepingu täitmine on pärast selle sõlmimist muutunud oluliselt raskemaks, võib raskustesse sattunud pool, keda ei ole käesoleva paragrahvi lõikes 2 nimetatud, nõuda halduslepingu muutmist vastavalt uutele oludele. Kui see ei ole võimalik või teine pool sellest keeldub, võib raskustesse sattunud pool pöörduda kohtusse halduslepingu lõpetamise taotlusega. Halduslepinguga antud õiguse lõpliku realiseerimisega võib tegu olla näiteks siis, kui isik on halduslepingu alusel saanud sihtotstarbelist toetust ning selle vastavalt otstarbele ära kulutanud.

Võrdluse ilmestamiseks võimaldab näiteks RHS § 8 lg 7 teine lause hankijal määrata ka rangema vorminõude, st kirjaliku, elektroonilise või notariaalse vormi. RHS kommentaaride järgi kui hankija seab riigihanke alusdokumendis sätestanud rangema vorminõude, kuid hankelepingu sõlmisel ei järgi seda vorminõuet, siis võib hankeleping olla tühine TsÜS § 83 lg

2 alusel.[125] Seega olukorras, kus elektroonilises vormis sõlmitud hankelepingule antakse elektrooniline allkiri, mis ei vasta allkirjastamise nõuetele, võib hankeleping osutada tühiseks. Mistõttu on oluline, et elektrooniline allkiri vastab regulatsioonidele ja antud allkirja tase vastab lepingu vorminõuetele. Samas on Riigikohtu praktikas asutud seisukohale, et allkirjastamise nõue ei ole igas olukorras pelgalt akti vormi küsimus ning sunnivahendit (s.o materiaalses mõttes halduse karistusotsust) ettenägev allkirjastamata haldusakt tuleb lugeda tühiseks HMS § 63 tähenduses.[126] Riigikohtu viidatud praktika kohaselt ei tähendanud allkirja puudumine seda, et haldusorgan poleks otsust selle andmise ajal teinud, vaid hiljem loeti algselt tehtud otsus tühiseks. Kuigi tühisuse tagajärjeks on, et otsus on kehtetu algusest peale (halduskohtumenetluse seadustik § 63 lg 1), ei muuda see otsust kui fakti olematuks. Mistõttu on avalikus sektoris ülimalt oluline, et nutilepingut kasutav haldusleping saaks vastava taseme allkirja tüübi.

[125] Simovart, M. A., Parind, Mart (2019) RHS § 8 komm p 63, lk 112.
[126] RKHKo nr 3-3-1-71-05, p-d 10 ja 13.

4. PLOKIAHELAL PÕHINEVA ALLKIRJA KASUTAMISE VÕIMALUSED

4.1. Elektroonilise allkirja regulatsioon ja käsitlus Eestis

Mõiste „elektrooniline allkiri“ (ehk e-allkiri) on laiem allkirja tüüp ja hõlmab erinevaid allkirjatasemeid – sealhulgas ka digiallkirju.[127] Eesti praktika järgi võib ekslikult jääda mulje, et digitaalallkiri on ainuke kõige tugevam allkirja vorm, kuid see ei vasta täielikult tõele. Elektroonilise allkirja aktsepteeritud määratlus on aga palju laiem kui „digitaalallkirja” määratlus ja nende vahel on olulisi erinevusi. Näiteks puutetundliku pliiatsi abil antakse elektroonilisele seadmele allkirju postipakkide kätte saamisel. Kuna e-allkiri ekraanil sarnaneb enamasti isiku omakäelise allkirjaga, tekib küsimus, kas tegemist võiks olla paberil antud omakäelise allkirjaga võrdsustatud allkirjaga. Sellist allkirja väljendusvormi peetakse elektrooniliseks allkirjaks ja on e-allkiri kõige üldisemas tähenduses. Tehniliselt pole vahet, kas allkiri antakse paberile või kasutades ekraani. Küll aga selliselt väljendatud allkirjal on mitmeid puudusi. Ilma tehnilise teabeta, kasutatavate protsesside ja tehnoloogiate kohta, ei anna e-allkiri mingit garantiid dokumendi allkirjastajast kolmandatele isikutele dokumendi sisu terviklikkuse. Elektrooniliste allkirjade peamine eelis on suurem kindlus allkirjastamise aja ja allakirjutanu isiku osas. Paberdokumendiga on alati see probleem, et sellele märgitud kuupäevi ei saa tegelikult usaldada. Mõned dokumendid võidakse tegelikult teha varem, mõned hiljem dokumendile märgitud kuupäevast. Elektroonilise allkirja formaadid kannavad endas ajatemplit, mis näitab, millal dokumendid on allkirjastatud. Samamoodi nagu eraõiguslike tehingute puhul on ka haldusõiguses allkirja eesmärgiks tõendada isiku tahet ning allkirjastaja ja allkirjastatu seost. Samas näeb haldusõigus õigusaktidele seadusest tulenevaid vorminõudeid, mis mõjutab ka antavat allkirja tüüpi ja taset.

Eestis tähistab mõiste **„**digitaalallkiri**“** (ehk digiallkiri, digiallkirjastamine jm) ainult sellist allkirjastamist tüüpi, mis on seaduslikult kehtiv ning juriidiliselt võrdne omakäelise allkirjaga. See tähendab, et kasutaja isik ja sertifikaadi väljaandja taust on kontrollitud ning allkirja andmise aeg on täpselt fikseeritud. Lihtsamalt öeldes on tuvastatud, kes allkirja andis, ning kindlustatud, et keegi kolmas ei ole allkirjastatavat dokumenti peale selle allkirjastamist muutnud. Eestis reguleerib e-identimist ja e-tehinguteks vajalikke usaldusteenuseid e-identimise ja e-tehingute usaldusteenuste seadus (edaspidi EUTS). Seaduses reguleeritakse neid aspekte e-identimise ja e-tehingute jaoks vajalike usaldusteenuste osas, mida määrus ei kata,

[127] ID. Digitaalne allkirjastamine ja elektroonilised allkirjad. Arvutivõrgus: https://www.id.ee/artikkel/digitaalne-allkirjastamine-ja-elektroonilised-allkirjad/ (5.04.2023).

või antakse võimalus reguleerida teatavaid valdkondi riigisisese õiguse alusel. Kuigi eIDAS määrus kasutab mõistet „kvalifitseeritud e-allkiri“ kui kõige kõrgema taseme allkirja, siis jätkati Eesti seadustes juba tuntud termini „digitaalallkiri“ kasutamist.[128] Mõistete seos on siiski sätestatud EUTS-is ja Eestis pidi seadusandja tegema valiku, kas muuta Eestis pikalt juurdunud termin „digitaalallkiri“ terminiks „kvalifitseeritud e-allkiri“. Tänu Eestis pikka aega kasutuses olnud ID-kaardi allkirjastamise lahendustele on Eestis tuntuks saanud mõiste „digitaalallkiri“. Eestis lahendati olukord selliselt, et EUTS-is loodi seos eIDAS määruse mõistete ja kehtetu digitaalallkirja seaduse mõistete vahel.

Oluline tähelepanek on see, et kuna määrus on vahetult kohaldatav, siis 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.[129] Tõsi, EUTS § 24 lg 1 kohaselt loetakse digitaalallkirja e-allkirjaks, mis vastab eIDAS määruse artikli 3 punktis 12 sätestatud kvalifitseeritud e-allkirja nõuetele, kuid mis see digitaalallkiri on, seda ükski Eesti seadus ei ütle. Siiski on Eesti seadustes kirjas erinevad digitaalallkirja mõisted, kuid seaduse sõnastuses ei ole eristatud elektroonilise allkirja tüüpe. Esmalt tuleks käsitleda allkirja funktsiooni. Tähtis ei ole allkirja tüüp (kui see ei ole seadusega ette nähtud), vaid see, kas seda rakendati viisil, mis viitas poolte soovile dokumenti autentida. Seejärel tuleks analüüsida olukordi, kus allkirja tüüp on seadusega ette nähtud. Allkiri peab võimaldama identifitseerida allkirjastanud isikut, samas seaduse sõnastus ei nõua omakäelise allkirja puhul nime lisamist. Peamine on isiku poolt antav unikaalne allkiri. Seadus ei näe konkreetselt ette, et allkiri peab olema inimesele loetav, vaid peab väljendama ainulaadset, vaid sellele isikule omast kirjakuju.

TsÜS kommentaaride autorid möönavad, et elektrooniline allkiri on laiem mõiste kui digitaalallkiri.[130] Nõustuti ka selles, et põhimõtteliselt on võimalik elektroonilist allkirja anda ka nt sõrmejälge või silma võrkkesta kasutades.[131] Järelikult saab eraõiguslikes tehingutes kasutada kõigi tasemete elektroonilisi allkirju. Juhul kui seaduses ei ole erinõuet, võib tehing olla allkirjastatud ükskõik millise taseme e-allkirjaga, et täita kirjalikku taasesitamist võimaldava vormi nõuded. Madalama tasemega e-allkirja puhul on elektroonilise vorminõude

[128] Seletuskiri e-identimise ja e-tehingute usaldusteenuste seaduse eelnõu juurde, 237 SE, lk 17–18. https://eelnoud.valitsus.ee/main#wmHbSe8s (19.04.2023).
[129] Kask, L., Laanest, K., lk 298.
[130] Varul, P., jt (2010). TsÜS § 80 komm, p 3.1., lk 250-251.
[131] *Ibidem*, TsÜS § 80 komm, p 3.1., lk 251.

täidetuks lugemiseks vaja kõrvaldada TsÜS § 78 lõike 1 ja § 80 lõike 1 vastuolu, mis peaks jääma seadusandja või kohtupraktika ülesandeks. TsÜS kommentaaridest ning eIDAS-määruse mõistetest lähtudes peaks ka madalama tasemega e-allkiri vastama elektroonilise vormi nõuetele, kuid TsÜS § 78 seaduse sõnastusest seda ei välja ei loe. Eelnevast saab järeldada, et kui halduslepingu puhul nõutakse kirjaliku lepingu vormi, mis nõuab omakäelist allkirjastamist. Selleks, et halduslepingu vastaks elektroonilises vormile, siis tuleb selleks anda ka elektrooniline allkiri. eIDAS artikkel 6 lg 1 järgi avalikus sektoris kasutatav e-allkiri peab vastama vähemalt täiustatud allkirja tüübile. Elektroonilise allkirja atribuuti ei ole täpsustatud, kuid autori hinnangul saab see olla elektrooniline allkiri, mis vastab täiustatud allkirja nõuetele). Elektroonilise allkirja atribuuti ei ole täpsustatud, kuid nii EUTS-i ja HMS-i järgid võiks asuda seisukohale, et õigusaktil peab olema digitaalallkiri. Samas HMS § 105 lg 1 võimaldab kohaldada TsÜS § 80 lg 3, sest halduslepingu puhul ei ole konkreetselt nõutud omakäelist allkirja vaid kirjaliku vormi. Autori hinnangul täidab haldusleping elektroonilise vormi nõude, kui sellele on antud elektrooniline allkiri. EUTS sätestab nõudeid kvalifitseeritud allkirjale, aga ei kõnele elektrooniliselt allkirjast laiemalt. eIDAS artikkel 26 nõuded täiustatud e-allkirjale on järgmised: see on seotud ainuüksi allkirja andjaga; selle abil on võimalk allkirja andja tuvastada; see on allkirjastatud andmetega seotud sellisel viisil, et kõik hilisemad andmete muudatused on tuvastatud. Täiendavalt on nõutud ka see, et see antakse e-allkirja andmiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures kasutada üksnes allkirja andja. Järelikult halduslepingule antav elektrooniline allkiri vastab eIDAS artiklile 26 ehk täiustatud e-allkirjale, siis saab eeldada ka TsÜS § 80 lg 3 nõude täidetavust.

4.2. Nutilepingu krüptograafilise allkirja vastavus halduslepingu vorminõudele

HMS § 99 lg 3 järgi sõlmitakse haldusleping kirjalikult. HMS § 5 lg-s 6 on sätestatud, et elektrooniline asjaajamine on haldusmenetluses võrdsustatud kirjaliku asjaajamisega, võttes arvesse elektroonilisest asjaajamisest tulenevaid erisusi. Digitaalallkirja ja e-templit kasutatakse haldusmenetluses e-identimise ja e-tehingute usaldusteenuste seaduses ning teistes õigusaktides sätestatud korras. Sellegi poolest on haldusmenetluses erinormidega võimalik määrata, kas menetlus toiminguks on vaja omakäelise allkirjaga võrdväärset allkirja või on võimalik kasutada ka madalama tasemega e-allkirja. Kõik dokumendid ja taotlused ei vaja kõige kõrgema tasemega allkirja ehk kvalifitseeritud e-allkirja.[132] Elektrooniliste allkirjade tasemete eristamine on oluline ja riigi kohustus avalike teenuste pakkumisel peaks olema ka

[132] Kask, L, lk 681.

selgitada isikutele, millised on menetluses eri tasemega elektrooniliste allkirjade kasutamise nõuded. Selliselt saavad pooled aru, milline õigusakt on oma vormilt õiguspärane ja milline mitte. Samuti võimaldab see menetluses kasutada madalama taseme allkirja ehk alati ei ole vaja asutuse juhi allkirja. See vähendab omakorda bürokraatiat ja kiireneb suhtus riigiga. Kuna ka madalama tasemega e-allkirjade puhul on isiku ja tema allkirja seos võimalik tuvastada, siis on tõendamisfunktsioon täidetud. Vastu võib väita, et riigi vaatest ei ole madalama taseme allkirjade kasutamine igal juhul variant, sest see võib vähendada usaldusväärsust riigi toimingute vastu. Mis jällegi ei vabasta avaliku teenuse pakkujaid selgitamast välja, millised on eri tasemega elektroonilise allkirja kasutamise nõuded ja õiguslikud tagajärjed. HMS § 107 kohaselt on peab toiming olema kooskõlas õigusaktidega. Toiming võib piirata õigusi või vabadusi ainult siis, kui selleks on seaduslik alus. Lõike 2 järgi toimingu sooritamise viisi, ulatuse ja aja ning menetlemise korra määrab haldusorgan oma äranägemisel, järgides kaalutlusõiguse piire ja võrdse kohtlemise ning proportsionaalsuse põhimõtteid.

Plokiahelal olevate nutilepingute puhul tekib küsimus, kas krüptovõtmega tehingu kinnitamine on võrdsustatav digiallkirjaga. TsÜS § 80 lg 3 järgi on allkirja funktsioon anda nõusolek tehingule, siduda tehingu teinud isikut ja oluline on ka allkirja andmise aeg. eIDAS artikkel 2 lg 3 sätestab, et määrus ei mõjuta siseriiklikku või liidu õigust, mis reguleerib lepingute sõlmimist ja kehtivust või muude juriidiliste või menetluskohustuste tekkimist ja kehtivust seoses vorminõuetega. Järelikult kui nutileping täidab lepingu vormi siseriikliku õiguses sätestatud eeldusi, siis on see leping selle riigi õiguse järgi kehtiv. Küll aga eIDAS seab regulatsioonid elektroonilise allkirja vormile.

Elektrooniline vorm nõuab kolme tingimuse täitmist. TsÜS § 78 järgi tuleb kirjaliku vorminõude täitmiseks dokument allkirjastada omakäeliselt. TsÜS § 80 lõike 1 kohaselt peetakse tehingu kirjaliku vormiga võrdseks elektroonilist vormi. Esiteks peab tehing olema tehtud püsivat taasesitamist võimaldaval viisil, teiseks sisaldama tehingu teinud isikute nimesid ja kolmandaks olema isikute poolt elektrooniliselt allkirjastatud. Siiski on TsÜS §-de 78 ja 80 vahel teatav vastuolu, sest kuigi elektroonilise vormi puhul on justkui võimalus kasutada ka madalama tasemega e-allkirju, siis kirjaliku vorminõude täitmiseks on dokument vaja allkirjastada üksnes omakäeliselt ehk elektroonilises keskkonnas kvalifitseeritud e-allkirjaga ehk digitaalallkirjaga. Vaatamata sellele, et enne eIDAS-määruse jõustumist Eestis eri taseme e-allkirju ei eristatud, on seadusandja leidnud, et digitaalallkiri on vaid üheks elektroonilise allkirja vormiks (TsÜS § 80 lg 3), millega ta on jätnud võimaluse kasutada ka teiste tasemete e-allkirju. Vastavalt seaduses nõutud vormi nõude järgi saab ka otsustada atribuudi taseme

määramisega.[133] L. Kase hinnangul on madalama taseme e-allkirja puhul on kindlasti täidetud kirjalikku taasesitamist võimaldava vormi nõue, mille puhul lähtuvalt TsÜS §-st 79 peab tehing olema tehtud püsivat kirjalikku taas esitamist võimaldaval viisil ja sisaldama tehingu teinud isikute nimesid, kuid ei pea olema omakäeliselt allkirjastatud.[134]

TsÜS § 80 lg 3 sõnastusest tulenevalt ei saa üheselt väita, et kas halduslepingul peab olema digitaalallkiri või piisab ka elektrooniliselt allkirjast, mille puhul ei pea olema tegemist kvalifitseeritud allkirjaga. Vastus ilmselt peitub HMS-s. HMS § 5 lg-s 6 mainitakse digitaalallkirja ja e-templi kasutatamist haldusmenetluses e-identimise ja e-tehingute usaldusteenuste seaduses ning teistes õigusaktides sätestatud korras. Ka HMS § 55 lg 4 järgi elektroonilisele haldusakti vormile ei pea lisama digitaalallkirja, kui haldusorgani juht või tema volitatud isik on turvalisel viisil tuvastatav. Eelnevast võib eeldada, et kuna HMS kõneleb ainult digitaalallkirjast kui kvalifitseeritud elektroonilisest allkirjast, siis ei ole muud elektroonilised allkirjad mõeldavad. Jällegi annab HMS 7. peatükk mitmeid sätteid, mille puhul tuleb halduslepingule kohaldada tsiviilõiguslikke sätteid, mis võimaldavad lähtuvalt TsÜS § 80 lg-st 3 kasutada elektroonilist allkirja. Seejuures ei ole seatud kohustuseks kasutada digitaalallkirja, vaid nähtud seda kui võimalusena. Autor on seisukohal, et kui antav elektrooniline allkiri täidab kõiki eeldusi, mis on ette nähtud HMS § 55 lg-s 4 vabastamaks dokumendilt allkirja andmist, siis sobib ka täiustatud e-allkiri eIDAS mõistes. Olenemata sellest saab jõuda siiski järelduseni, et nutilepingu vormis olev haldusleping täidab seaduses sätestatud vorminõudeid, kui sellele antakse kvalifitseeritud elektrooniline allkiri ehk digitaalallkiri. Tehnoloogia pakub võimalust kasutada nutilepingu vormi, aga sellele peab lisanduma plokiahela väline allkiri.

4.3. Krüptograafilise allkirja vastavus eIDAS elektroonilise allkirja tüüpidele

Tsentraliseeritud lahendus tähendab tsentraliseeritud sertifitseerimisasutust ja see tähendab tsentraliseeritud üksust, mis haldab kasutatavate võtmete turvalisust. Tsentraliseeritud üksusete puhul peamiselt PKI-lahenduste kasutamine muudab lahenduse haavatavaks selliste rikkumiste suhtes, nagu ühe tõrkepunkti või keskasutuste rünnakud. See toob esile vajaduse, aga ka valmisoleku otsida muid lahendusi, mis seda haavatavust väldivad, kuid millel on ka muid eeliseid. Detsentraliseeritud lahendusel, näiteks plokiahelal, seda turvariski ei ole ja just see asjaolu on pakkunud paljude isikute jaoks suurt huvi. Raskus seisneb selles, et praegu ei saa seda rakendada, et järgida olemasolevat eIDAS-i, mis takistab elektroonilise identifitseerimise

[133] Kask, L, lk 680-681.
[134] *Ibidem.*

kasutamist ELi piiriüleselt, kuid selleks võiks kasutusele võtta määruse ajakohastatud versioonis. Tehniliselt on PKI mudelil ja DLT-l põhinevad allkirjastamisprotsessid üsna sarnased.[135] Kuna DLT on tehnoloogiate fusioon, seob see selliseid tehnoloogiaid nagu krüptograafia, P2P-võrgud, konsensusmehhanism ja seotud ajatemplimine ilma tsentraliseeritud usaldusstruktuure kaasamata, kasutades siiski suures osas sama tehnoloogiat nagu PKI mudel. Lisaks loob usaldus tehnilise seadistuse ja auditeeritava protokolli vastu detsentraliseeritud usalduse, ilma et oleks vaja kaasata LOTL-põhiseid tsentraliseeritud usaldusteenuse pakkujaid.[136] Hajussüsteemis nutilepingu kasutaja tuvastamiseks on vajalikud era- ja avalikud võtmed. Need võtmed toimivad kui autentimisena, et ühel kindlal kasutajal on volitused toimingu tegemiseks.[137] Võtmeid ei loo ega halda allakirjutanu nimel usaldusteenusteenuse pakkuja ja seetõttu puudub vajadus usaldusteenuse pakkuja sellesse protsessi kaasata.[138] Nutilepingu arvutikood kasutab rahakotti aadressi ühendamiseks seda avaliku võtmega. Autori arusaam on, et kui võtmeid kasutatakse elektroonilisel allkirjastamisel nutilepingul, mis on seotud ainult kasutaja valduses olevate võtmetega, siis ei ole vaja võtmeid võtmetena väljastada eraldi usaldusteenuse pakkuja poolt. Vaid allkirjasta identifitseerimisel lähtutakse sellest, kelle käes on võtmed. Sama põhimõte, kui keegi kasutab ID-kaardile väljastatud PIN-koode. Siiski oleks autori hinnangul vaja tagada, et väljastatud võtmed saavad olla seotud ainult ühe isikuga.

eIDAS elektrooniliste allkirjade regulatsioon on üles ehitatud LOTL infrastruktuuri ja PKI mudeli ümber. DLT on tehnoloogiate liit, mis seob omavahel krüptograafia, P2P-võrgud, konsensusmehhanismi ja seotud ajatempli, kuid ei hõlma tsentraliseeritud usaldusstruktuure. DLT-protokollil põhinev osapoolte vaheline suhtlus on krüpteeritud ja kasutab lingitud ajatemplit, mis on funktsionaalselt samaväärne eIDAS-e alusel elektroonilise allkirjastamisega. Lisaks kasutatakse DLT-põhises lepingus sarnast avaliku ja privaatvõtmega krüpteerimisalgoritmi, nagu on nõutud eIDAS-e koostalitlusvõime raamistiku alusel ELi tehnilistes standardites.[139] Hajussüsteemil võib nutilepingus määrata, et autentimise eesmärgil loodud tõendi kontrollimiseks saab kasutada teatud kontrollimeetodit, nagu krüptograafiline avalik võti või pseudonüümne biomeetriline protokoll. Detsentraliseeritud identifikaator on palju rohkem identiteedi ja juurdepääsu haldamise kontseptsioon, kus ühelt poolt otsustab identiteedi omanik, kellele ta millise osa oma identiteediinfost annab ja teisest küljest ei pea

[135] Veerpalu, A. jt, lk 31.
[136] Veerpalu, A., lk 143.
[137] Eenmaa, H., Schmidt-Kessen, M. J. Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts, lk 21.
[138] Veerpalu A., lk 142.
[139] *Ibidem*, lk 147.

andma kõigil juhtudel täielikku identiteediinfot, vaid ainult vajaliku osa. Turvaline digitaalne isikutuvastus ja (kvalifitseeritud) usaldusteenuse olemasolu on ühed peamised nõuded lubanaks hajussüsteemidel põhinevat allkirjastamist. Praktikas peaks neid detsentraliseeritud identifikaatorid kasutama koos isikut tõendava teabega, mis muudab lihtsamaks digitaalse info vahendamise kolmandate osapooltega.

PKI mudel on mudel üksikisikute ja muude objektide (nt veebisaitide) usaldusväärsete elektrooniliste identiteetide haldamiseks. Mudeli komponendid on standardid, tehnoloogia ja protseduurid. Mudel sõltub digitaalsetest sertifikaatidest, mille loovad, levitavad, tühistavad ja haldavad keskhaldussüteemi pidajad. Nad on kolmandad osapooled, kes on spetsialiseerunud identiteedi ja avaliku võtme vahelise ühenduse kinnitamisele allkirjastatud sertifikaadi väljastamise kaudu. See sertifikaat kinnitab seost identiteedi ja avaliku võtme vahel.[140] Iga kord, kui elektroonilisi allkirju kasutatakse, on nende kehtivus juba tunnistatud piisavalt turvaliseks näiteks siseturul elektrooniliste tehingute elektroonilist identifitseerimist ja usaldusteenuseid käsitleva määruse (eIDAS määrus) reguleerivas raamistikus. Kui aga sellised kaitsemeetmed puuduvad, ei ole ahelaväliste formaalsete nõuete eesmärk täidetud või e-allkirjad ei ole eIDAS-e määrusega nõutud viisil kaitstud, ei saa plokiahela tehingud ja nutikad lepingud seda rolli täita.

Usaldusteenuste pakkujate poolt sertifikaatide ja isiklike võtmete väljastamine on vajalik, et allkirja saaks pidada kvalifitseeritud elektrooniliseks allkirjaks. See tagab selle, et lepingut saaks lugeda elektroonilises vormis lepinguks. Nutilepingut kasutatava hajussüsteem kasutab teistmoodi usaldustaristut. Esiteks ei hõlma hajussüsteemil põhinev nutileping usaldusteenuse pakkujaid ja ei väljastata sertifikaate.[141] See tähendab, et kuigi hajussüsteemi põhine allkiri ei kasuta PKI mudeli sertifitseerimist ega CA lahendust, on identifitseerimisfunktsiooni täitmiseks mitmeid lahendusi. Nutilepingu puhul on see ehitatud selle protokolli ja toimimis reeglitesse.[142] Avaliku võtme vastutava töötleja identiteeti saab siduda rahakoti aadressiga läbi eraldi identifitseerimisprotsessi. Nagu ka seda, kes oma privaatvõtmega avalikku võtit kontrollib, loetakse tehingu allkirjastajaks ja ahelaväline või ahelasisene identiteedi sidumine võtmepaariga võimaldab identiteedi siduda elektroonilise allkirjaga. Kui nutilepingu sõlmimisel kasutatud võtmed on seotud mittehalduri rahakotiga, genereerib võtmed protokoll, mitte keskhaldusüksus ise.[143] Järelikult, et kaaluda muude mitte PKI mudelipõhiste

[140] Veerpalu, A. jt, lk 34.
[141] *Ibidem*, lk 39.
[142] Domingo, I. A., lk 19.
[143] *Ibidem*, lk 132-135.

autentimistehnoloogiate kasutamist, peab regulaator hindama, kas mis tahes PKI mudelile üles ehitatud regulatsioon on tõesti avatud uuele, vähem sertifitseerimiskesksele autentimistehnoloogiale.

Sellest tulenevalt ei ole tehnilisi piiranguid turvaliste elektrooniliste ajatemplite rakendamisel plokiahela plokile ja laiemalt kogu plokiahelale. Siiski tekib küsimus, kas selline lähenemine vastab eIDAS määruse nõuetele kvalifitseeritud elektroonilistele ajatemplitele. eIDAS määruse artikkel 42 lg 1 sätestab kolm nõuet. Seda võiks ületada sellega, et kõigepealt saadetakse sisu (nt rendiauto foto) räsiväärtus usaldusväärsele kolmandale osapoolele või usaldusteenuse pakkujale (eIDAS terminoloogias). Teiseks lisab usaldusväärne teenusepakkuja praeguse kuupäeva ja kellaaja, allkirjastab saadud andmed ja edastab tulemuse oma kliendile[144] Viimaseid (st elektroonilisi ajatempleid, mis ei vasta kvalifitseeritud elektrooniliste ajatemplite nõuetele) nimetame lihtsateks elektroonilisteks ajatempliteks. Näiteks on foto- või videofailis metaandmetena lisatud teave kuupäeva ja kellaaja kohta, moodustab see teave juba lihtsa elektroonilise ajatempli.[145] Ühelt poolt kuupäeva ja kellaaja ning teiselt poolt andmete sidumine peab olema turvaline, st andmete muutmatus peab olema mõistlikult välistatud (EIDAS määruse artikkel 41 lg 1 järgi). Ajatempel peab põhinema "täpsel ajaallikal, mis on seotud koordineeritud universaalajaga".

Lõpuks allkirjastab selle kvalifitseeritud usaldusteenuse pakkuja, kasutades täiustatud elektroonilist pitsatit, täiustatud elektroonilist allkirja või samaväärset meetodit. Andmed on elektroonilisel kujul, mis seob muud elektroonilisel kujul olevad andmed teatud ajahetkega, mis tõendab, et viimased andmed olid sel ajal olemas (eIDAS määrus artikkel 3 p 33). Andmed peavad olema seotud kindla ajaga. Bitcoini plokiahel on üles ehitatud nii, et uus plokk genereeritakse keskmiselt iga 10 minuti järel. Plokkide genereerimisel on juhuslik element. Kui on oluline tõestada, et andmed on teatud minuti jooksul olemas olnud, on Bitcoini plokiahel seetõttu sobimatu.[146] Kvalifitseeritud elektroonilist ajatemplit ei ole võimalik saavutada, et järgida kehtivat eIDAS nõudeid. Artikli 41 lg 2 puudutab selles märgitud kuupäeva ja kellaaja täpsust ning nende andmete terviklikkust, millega kuupäev ja kellaaeg on seotud. Artikli 42 lõiget 1 – mis tähendab eeldust, et elektrooniline ajatempel loetakse kvalifitseerituks – ei saa

[144] Sorge, C., Leicht, M. Blockchain-based electronic time stamps and the eIDAS regulation: The best of both world. – Scrpited, Volume 19, Issue 1, Feburary 2022, lk 75.
[145] Sorge, C., Leicht, M., lk 70.
[146] Sorge, C., Leicht, M., lk 74.

esitada ilma artiklis 4 nimetatud vastava rakendusaktita.[147] Aga läbi tehniliste lahenduste võib seda ikkagi saavutada, nt siduda metaandmetega kuupäev ja kellaaeg.

Eestis kasutatav BDOC allkirjavorm põhineb ASiC konteineri ja XAdES allkirja standarditel (ASiC konteiner-failiformaat, mille sees on kasutatud XAdES (XML) allkirja). DigiDoc klienditarkvaras saab anda nii siseriiklikke BDOC- kui ka Euroopas tunnustatud ASiC-E-vormingus digiallkirju. Viimast tuleks eelistada, kui soov on saada allkiri, mis on võrdne Euroopa Liidus omakäeliselt antud allkirjaga. Allkirja andmise aja fikseerimiseks kasutatakse kolmanda osapoole aega, mille fikseerimiseks saab eelnimetatud standardite kohaselt kasutada kas ajamärgendit (ingl *timemark*) või ajatemplit (ingl *timestamp*). Kuna Eesti digitaalallkiri on vanem kui ajatempel[148], siis ajaloolistel põhjustel on tänaseni Eestis enimlevinud lahenduseks ajamärgend, kus allkirjastatavad andmed seotakse sertifikaadi kehtivuspäringuga ning päringu vastuse kellaaega tõlgendatakse kui ajamärgendit.[149] Selleks on nõutud, et allkirja sertifikaadi staatus ja kehtivus peavad olema kontrollitavad ja seotud allkirja andmise ajaga. eIDAS määrusega kehtestatud kohustuslikud standardid pakuvad ainsa usaldusväärse meetmena digiallkirjastamise aja määramiseks kvalifitseeritud ajatempli teenust. Seega on digitaalallkirja kehtivuse tuvastamiseks vajalik ajatempli olemasolu.

Eesti enda loodud ajamärgendi uuendamiseks võeti kasutusele KSI Blockchain ajatempel. KSI Blockchain pakub teenusena verifitseerida oma andmeid riigiasutuste andmebaasides.[150] KSI Blockchain annab võimaluse igale selle kasutajale kontrollida oma kasutatud andmete vastavust riigi andmebaasides, vastavuse tagamine langeb riigile endale. Andmete pikaajaline säilitamine on võimalik tänu räsifunktsiooni[151] (ingl *hash*-funktsion) krüptograafiale, mis muudab selle elektroonilise allkirja palju turvalisemaks võrredes PKI-ga.[152] Tuntumad usaldusteenused on näiteks Smart-ID, mobiil-ID ning Eesti Vabariigis väljastatavale ID-kaardile elektroonilise isikutuvastuse ja allkirjastamise sertifikaatide väljaandmine. Eestis on käesoleval hetkel kaks

[147] Sorge, C., Leicht, M., lk 78.
[148] e-ajatempel on elektroonilised andmed, mis seovad muud elektroonilised andmed kindla ajahetkega ja tõendavad, et viimatinimetatud andmed olid sel ajahetkel olemas (eIDAS artikkel 3 p 33).
[149] Erlich, M. Riigi Infosüsteemide Amet. E-Allkirjad Euroopas ja nende käsitlemine Eestis. Arvutivõrgus: https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/usaldusteenused-ja-koostoo (12.03.2023), lk 3-4.
[150] E-Estonia. Arvutivõrgus: https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf (12.01.2023).
[151] Räsimine on ühesuunaline krüptograafiline funktsioon, mis muudab mis tahes teksti loetamatuks stringiks numbrid ja tähed, mis on kordumatud ja tagavad järelikult räsitud teksti muutmise koos. Tegemist on nagu ketiga, mis ühendab plokiahela plokke. Vt peatükki 1.1.
[152] Eenmaa-Dimitrieva, H., Schmidt-Kessen M.J. Regulation through code as a safeguard for implementing smart contracts in no-trust environment, lk 21-22.

usaldusteenuse pakkujat: GuardTime OÜ and SK ID Solutions AS.[153] Kvalifitseeritud usaldusteenuse pakkuja kontrollib allkirja, mis tagab muuhulgas sisu terviklikkuse, allkirjastamise aja selguse ja allkirjastaja isikusamasuse.

Kokkuvõttes saab öelda, et hajussüsteemi ei ole võimalik kasutada usaldusväärsete digitaalsete tehingute jaoks, kui ei ole kasutusele võetud vastavaid turvameetmeid eIDAS-st lähtuvalt. Hajussüsteemil kasutatavaid detsentraliseeritud identifikaatoreid ei saa kasutada, kuni puudub usaldusallikas ja selle mandaatide kontrollitav autentsus.

4.3.1. Krüptograafilise allkirja vastavus täiustatud elektroonilise allkirja tüübile

Praktikas eksisteerib kolme tüüpi elektroonilisi allkirju: lihtne elektrooniline allkiri (ingl *Simple Electronic Signature* ehk SES), täiustatud elektrooniline allkiri (AES) ja kvalifitseeritud elektrooniline allkiri (QES). eIDAS tunnustab nii AES kui ka keerukamate ja turvalisemate vorme QES elektroonilisi allkirju. [154]

eIDAS artikli 3 p 11 järgi täiustatud e-allkirjad kvalifitseeritud sertifikaatidega (AdES/QC) on täiustatud e-allkirjad, mis põhineb eIDAS artiklis 26 sätestatud nõuetele. Täiustatud elektroonilised allkirjad põhinevad küll kvalifitseeritud sertifikaadel, kuid ei kasutata kvalifitseeritud allkirja andmise vahendit. See tähendab, et allkirjastamise andmed (privaatvõti) võib olla paigaldatud näiteks kasutaja arvutisse. Samas võib võti olla ka kiipkaardil, kuid seda vahendit ja selle loomist pole auditeeritud ega sertifitseeritud (puudub garantii). Täiustatud allkirjaga on võimalik täida eeldus, milleks on seos allkirjastatud dokumendi ja allkirjastaja vahel.[155] AES tüübi allkirja funktsioonideks on järgnev: a) allakirjutanuga unikaalselt seotud; b) peab suutma allkirja andjat tuvastada; c) peab olema antud e-allkirja andmiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures kasutada üksnes allkirja andja ja see peab olema allkirjastatud andmetega seotud sellisel viisil, et kõik hilisemad andmete muudatused on tuvastatavad.

Allakirjutanuga unikaalselt seotud funktsiooni tagamiseks on usaldusteenuse pakkujad. EUTS § 5 lg 3 järgi kvalifitseeritud usaldusteenuse osutaja dokumenteerib usaldusteenuse osutamisel tehtud toimingud ning säilitab sellekohast tegevuslogi kümme aastat kirje loomisest arvates.

[153] SK ID Solutions AS koduleht. Arvutivõrgus: https://www.skidsolutions.eu/ettevottest/ (20.04.2023).
[154] Law Commission. Smart legal contracts, lk 65-66.
[155] Kask, L., lk 677.

EUTS § 5 lg 5 sätestab, et kvalifitseeritud usaldusteenuse osutaja tuvastab enne kvalifitseeritud sertifikaadi väljastamist isikusamasuse, kontrollib seda isikut tõendavate dokumentide seaduse § 2 lõikes 2 nimetatud dokumendi, välisriigis väljastatud kehtiva reisidokumendi või isikut tõendavate dokumentide seaduse § 4 lõikes 1 sätestatud tingimustele vastava muu dokumendi alusel ning kontrollib esitatud teabe usaldusväärsust. Juriidilisele isikule sertifikaadi väljastamisel kontrollib usaldusteenuse osutaja lisaks esindusõiguse olemasolu. Seega usaldusteenuse pakkujate funktsioon on võtmete ja sertifikaatide genereerimine ja väljastamine, et siduda võtmed nii tõendus- kui ka identifitseerimisfunktsiooni täitvate isikutega. DLT-põhiste allkirjade puhul ei genereeri ega väljasta DLT võrgus osalejad elektrooniliseks allkirjastamiseks vajalikke võtmeid ega seo võtmeid isikuga allkirja andmise kaudu digitaalsed sertifikaadid. Nutilepingu kasutamisel on võimalik rahakotisüsteem, kus selle kasutaja kontrollib nii era- kui avaliku võtit. Seda sama põhimõtet nõutakse ka PKI mudelipõhistel allkirjadel, mistõttu lugeda täidetuks ka nutilepingu ainulaadne seostatus allkirjastajaga.

Allkirjastaja identifitseerimise nõude osas ei tohiks samuti probleeme esineda. Nutilepingu puhul ei ole kõigi allakirjutanute identiteet lepingu ja selle allkirjastamisprotsessiga otseselt seotud. Küll aga võib ka lähtuda peamiselt sellest, et kes iganes kasutas krüptograafilist allkirja, saab pidada allkirja andjaks. eIDAS määruse artikkel 3 p 25 järgi on autentimine elektrooniline protsess, mis võimaldab isikute e-identimist või elektrooniliste andmete päritolu ja tervikluse kinnitamist. Üldjuhul on autentimistehnoloogia ülesehitatud järgides põhimõtetet: a) midagi, mis kellegil on; b) midagi, mida keegi on või c) midagi, mida keegi teab. EL-i riikide elektroonilised allkirjastamise süsteemid on tavaliselt üles ehitatud a) ja b) variandile nagu Eestis on kasutatav Digidoc tarkvara.[156] Oluline on siiski teadmine, et kes on see isik tegelikult. Nagu magistritöös eelnevalt on välja toodud, siis identifitseerimisfunktsiooni saab täita plokiahela väliselt, kasutades selleks hajussüsteemi pakkuja autentimist või krüptodevarade puhul sarnase rahakotiteenuse pakkuja autentimist.

Seega kasutades laialt levinud AES-i (nt DocuSign[157], PandaDoc[158]) on võimalik tuvastada allkirjastamise aega ja tagada dokumendi sisu muutumatuks jäämine, kuid kuna puudub vahepealne kvalifitseeritud usaldusteenuse pakkuja, siis praktikas ei ole võimalik olla kindel

[156] Veerpalu, A. jt, lk 32.
[157] DocuSign veebileht. Arvutivõrgus: https://www.docusign.com/ (19.04.2023).
[158] PandaDoc veebileht. Arvutivõrgus: https://www.pandadoc.com/electronic-signature-software/?utm_source=google&utm_medium=cpc&utm_campaign=Google_Search_NB_Competitor_EU&utm_content=DocuSign&utm_device=c&utm_placement=&utm_term=docusign&utm_creative=613599673654&gclid=Cj0KCQjwlumhBhClARIsABO6p-wL34m1WkUzq09peOubWHCgegqiTcZh-JMvsFZMTYNDsqqguTo1lJcaAj3DEALw_wcB (19.04.2023).

allakirjutanu isikus. Näiteks võib allkirjastamiseks kasutatav e-posti aadress olla fiktiivne või e-posti aadressi võib kasutada pahatahtlik kolmas osapool. Seetõttu ei saa AES-i pidada omakäelise allkirjaga samaväärseks elektrooniliseks allkirjaks. Tõsi, maailmas on palju erinevaid e-allkirja formaate, ent kuna nende tunnustatavus ja kasutatavus Eestis peab olema seadusega reguleeritud, siis mitte iga allkirja tüüp ei tule kõne alla avalikus sektoris kasutamisel. Seaduslikkuse tingimusele vastavad aga kõik e-vormid, mida sätestavad eIDAS ja EUTS. Sellest olenemata eIDAS määrus artikkel 25 lg 1 järgi e-allkirja ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud e-allkirjadele esitatavatele nõuetele. Täiustatud allkirja puudub küll kvalifitseeritud allkirjastamis vahend, kuid täidab allkirjastamise funktsioone nagu isiku seostamine tehingu tegijaga ja dokumendi tõendamine. Seega autori hinnangul ei too nutilepingu vormingus halduslepingule antud täiustatud allkiri kaasa veel lepingu tühisust.

4.3.2. Krüptograafilise allkirja vastavus kvalifitseeritud elektroonilise allkirja tüübile

Kvalifitseeritud e-allkirjad (QES – *qualified electronic signature*) on määruse mõistes võrdsed omakäelise allkirjaga. Sellised allkirjad on täiustatud e-allkirjad (kirjeldus ülejärgmises punktis), mis põhinevad kvalifitseeritud sertifikaatidel (kvalifitseeritud sertifitseerimisteenuse osutaja poolt väljastatud) ja on antud kvalifitseeritud allkirjaandmise vahendiga (varasemalt tuntud kui turvaline allkirja andmise vahend). Euroopa Liidus peab QES-il olema sama õiguslik mõju kui omakäelisel allkirjal. See tähendab, et kui tehingule kohaldatav seadus nõuab dokumendi käsitsi või digitaalset allkirjastamist, tähendab see kvalifitseeritud elektroonilist allkirja. Teisisõnu, seni kuni elektroonilise allkirja andmise vahend ei ole kvalifitseeritud, ei saa rääkida omakäelise allkirjaga samaväärsest elektroonilisest lahendusest. Kvalifitseeritud allkiri peab sisaldama allkirjasertifikaati, sertifikaadi väljaandja ja sertifikaadi väljastaja peab olema Euroopa Liidu kvalifitseeritud usaldusteenuse pakkuja (talle on antud QES sertifikaat). Kui kõik need asjaolud on tuvastatavad, on tegemist kvalifitseeritud elektroonilise allkirjaga. Kui sellist sertifikaati on keeruline leida või pole selge, kas tegemist on QES-iga, tuleks pigem eeldada, et tegemist pole kvalifitseeritud elektroonilise allkirjaga.

Kvalifitseeritud sertifikaat on kui garantii, et sertifikaadi väljastamisel tuvastati füüsilise isiku identiteet. Kvalifitseeritud allkirja andmise vahend on kui garantii, et allkirja loomiseks kasutatavad andmed (privaatvõti) on kindlalt allkirjastaja ainukontrolli all. eIDAS artikli 3 lõige 15 sätestab, et elektroonilise allkirja kvalifitseeritud sertifikaat on kvalifitseeritud usaldusteenuse osutaja väljastatud ja eIDAS I lisas sätestatud nõuetele vastav elektroonilise

allkirja sertifikaat. Kehtestatud viisil on need nõuded suunatud tõendamis- ja identifitseerimisfunktsiooni täitmisele ning autori poolt on analüüsitud, et neid mõlemaid funktsioone saab täita nutilepingus kasutatavate alternatiivsete lahendustega. eIDAS-e artikli 3 lõige 23 viitab kvalifitseeritud elektroonilise allkirja andmise seadmele tarkvarale või riistvarale, mida kasutatakse elektroonilise allkirja loomiseks ja mis peab vastama eIDASe II lisa nõuetele. Vastavalt eIDAS artikkel 3 p-le 23 peavad kvalifitseeritud e-allkirja andmise vahendid vastama eIDAS lisas II sätestatud nõuetele. Nutileping on võimeline täitma kõiki eelnevaid nõudeid, kuid probleem ilmneb lõike 3 osas. Lisa lg 3 järgi e-allkirja andmiseks vajalikke andmeid võib allkirja andja nimel luua või hallata üksnes kvalifitseeritud usaldusteenuse osutaja. Tegemist on ühe peamise takistusega võrdsustamaks nutilepingute kürptograafiliste võtmete kasutamist kvalifitseeritud allkirja tüübiga.

Kvalifitseeritud elektroonilise pearaamatu peab koostama vähemalt üks kvalifitseeritud usaldusteenuse pakkuja. See peab tagama nii pearaamatusse kantud andmekirjete õige järjestuse kui ka andmete õige järjestikuse kronoloogilise järjestuse pearaamatus ning andmete sisestamise kuupäeva ja kellaaja täpsuse. Peale selle peab ta andmed salvestama nii, et kõik hilisemad andmete muudatused oleksid koheselt tuvastatavad. Kvalifitseeritud elektroonilise pearaamatu puhul eeldatakse selles sisalduvate andmete ainulaadsust ja autentsust, nende kuupäeva ja kellaaja täpsust ning nende järjestikust kronoloogilise järjestust pearaamatus.[159] Digitaalallkiri on teatud tüüpi elektrooniline allkiri, mis on loodud asümmeetrilise või avaliku võtmega krüptograafia abil.[160] Lepingu asukoht või paigutamine nutilepingute puhul on lihtne, sest leping asub andmebaasis kus leping sõlmiti. Seega nutilepingute puhul, mis asuvad plokiahelas, on lihtne neid hoiustada ja mis tagavad korrektse kokkulepe sõlmimise aja.[161] Hajusraamatutehnoloogia põhiste elektrooniliste allkirjade usaldusväärsus ei sõltu usaldussertifikaatidest ega usaldusteenuse pakkuja väljastatud privaatvõtmetest just seepärast, et võtmed, mida kasutatakse hajusraamatutehnoloogiale tuginevas allkirjastamisprotsessis (olenevalt kasutaja eelistustest), väljastab protokoll otse kasutajale. Seega, erinevalt PKI-mudelist puudub hajusraamatutehnoloogia puhul vajadus usaldusväärse vahendaja või ametiasutuse järele, kes neid allkirjastamiseks vajalikke võtmeid keskselt väljastaks ja haldaks. See siiski ei tähenda, et kõikidele hajusraamatutehnoloogiat kasutavatele tarkade lepingute kasutajatele saaks kinnitada, et see protokoll on funktsionaalselt samaväärne eIDAS-e elektroonilise allkirja protokolli ja usaldussüsteemiga. See on peamine puudus, miks

[159]Euroopa Komisjoni ettepanek, p 41.
[160] Law Commission. Smart legal contracts, lk 64-65.
[161] Idelberger, F., lk 175.

hajussüsteemil põhinev nutileping ei täida kvalifitseeritud allkirja nõudeid, sest tal puudub usaldusteenuse osutaja. Vastavaid võtmeid luuakse nutilepingu protokollis endas.

Võttes arvesse, et Eestis juba kasutatakse eIDAS-ile vastavat krüptograafilist allkirjastamist KSI Blockchain poolt, siis krüptograafiline allkirjastamine vastab kvalifitseeritud elektroonilisele allkirjale. Väidetavalt ei ole KSI Blockchain lahendus täielikult hajussüsteemi põhine, vaid kasutab erinvaid tehnoloogia segunemisi vastamaks eIDAS nõuetele. Hajussüsteemil põhinev krüptograafiline allkiri ei sõltu usaldusteenuse pakkujast. Analüüsi käigus ilmnes, et hajussüsteemil põhinev nutilepingu allkirjastamise tüüp ei täida eeldusi kvalifitseerimaks usaldusteenuste pakkuja nimekirja LOTL-i ja digitaalseid sertifikaate ka ei väljastata. Eelnevast tulenevalt saab asuda seisukohale, et plokiahela tehnoloogia tehnilisest küljest täidab kõiki eIDAS ja Eesti seadustest määratletud halduslepingu vormi nõudeid. Vastupidiselt avalikule sektorile saab erasektor ise otsustada, kas ja millise turvalisuse tasemega e-allkirju aktsepteerida. Küll aga eIDAS ei tunnista neid allkirju kvalifitseeritud elektrooniliste allkirjadena. Mistõttu EUTS mõttes ei saa seda võrdsustada ka omakäelise allkirjaga. Halduslepingu puhul on seadus ettenäinud küll kirjaliku vorminõude, millest tulenevalt nõutakse omakäelisega võrdset allkirja ehk kvalifitseeritud allkirja nõuet täitvat digitaalallkirja, siis tulenevalt halduslepingust kui sooritavast haldusest, saaks autori hinnangul lepingu pooled vabalt leppida kokku ka madalamataseme allkirja kasutamises.

Siinkohal autor ei eeldagi, et haldusasjaajamine saabki olema ainult e-infosüsteemides. Eestis leidub veel kindlasti pikemat aega elanikkonnagruppe, kelle jaoks paberil ja kohapeal asjaajamine on eelistatum (nt pensionärid). Küll aga saab haldusorgan seada endale eesmärgiks muutuda paberivabaks enda toimingutega. See on samuti üks eesmärke ja kasutegureid liikudes detsentraliseeritud keskkonna poole. Infosüsteemi vahendusel dokumentide esitamine on suur hüpe selle poole, et vähendada üleliigset allkirjastamist dokumentidel. Madalama taseme allkirja kasutamise võimalus peaks teoreetiliselt vähendama bürokraatiale kuluvat aega, sest mitte iga dokument ei pea saama kõrgelt kvalifitseeritud digiallkirja ja seda veel haldusorgani juhilt. Sellest olenemata ei ole välistatud, et haldusorgani siseselt on töökorraldustest jätkuvalt ettenähtud digiallkiri. Haldusorganid võiksid eristada, millistele haldusorgani poolt antud dokumentidele on vajalik madalama või kõrgelt kvalifitseeritud elektrooniline allkiri ning infosüsteemi kasutamise võimalusel vähendada iga dokumendi allkirjastamise vajadust.

KOKKUVÕTTE

eIDAS määruse tulek on tõstatanud küsimuse identifitseerimist pakkuvate teenuste osutamist uute tehnoloogiatega, nt hajussüsteem ja plokiahel. Plokiahela tehnoloogia laialdasem kasutamine on endaga kaasa toonud automatiseeritud tehingud, milles kasutatakse nutilepingute nimetuse all tuntuks saanud lahendusi. Nutilepingu on kokkuleppeid täideviiv tarkvara, mis kasutab hajussüsteemil põhinevaid tehnoloogilisi lahendusi. Nutilepingu kasutamist võib käsitleda ka kui digikonteinerina, kuhu lisatakse tehingu sisu kirjeldav osa, kuid mille vormi ja allkirjastamise eeldused täidab konteiner ise. Plokiahelal põhinevate nutilepingute puhul tekib küsimus, kas need lepingud on käsitletavad lepingutena Eesti seaduste mõistes ja kas krüptovõtmega tehingu kinnitamine on võrdsustatav Eestis kasutatava digiallkirjaga, kui tehingu vorm on seadusest tulenev?

Magistritöö põhieesmärgiks oli analüüsida plokiahela tehnoloogiat kasutava nutilepingu vastavust vorminõuetele halduslepingu näitel ja sealhulgas leida, millised on hajusraamatu tehnoloogial põhineva elektroonilise allkirja taseme kasutamise võimalused kehtiva haldusmenetluse seaduse alusel. Vaatamata sellele, et lepinguõiguse üldprintsiibi järgi on lepinguvorm vaba, on vaja uurida, kas nutilepingud täidavad traditsioonilise lepingu kriteeriume kehtivas õiguses. Eestis on nutilepingute sobivus kui eraldi vormina siseriikliku õiguse järgi suures osas analüüsimata ning selle teemalist eestikeelset kirjandust on veel vähe. Sestap on vajadus uurida kehtiva regulatsiooni ning võimalusi tõlgendada nutilepinguid lepingutena. Autor analüüsis, kas plokiahelal põhinevad nutilepingud on käsitletavad lepingutena Eesti seaduste mõistes ja kas krüptovõtmega tehingu kinnitamine on võrdsustatav Eestis kasutatava digiallkirjaga, kui tehingu vorm on seadusest tulenev. Töö fookuses oli avalikus sektoris kasutatav halduslepingu, kus lepingu vormidele on seadusest tulenevad kohustuslikud vorminõuded, sh allkirja kohustuslikkuse nõue. Autor lähtus analüüsi tegemisel peamiselt halduslepingu formaalse eeldustest. Haldusmenetluse seaduse (edaspidi HMS) § 99 lg 3 järgi sõlmitakse halduslepingu kirjalikult. Haldusõiguses tuleb halduslepingute puhul vastavalt juhtumile halduslepingu vormi täitmist hinnata tsiviilõiguslike lepingute jõustumiseks ettenähtud korras, arvestades HMS-ga kehtestatud erisusi (HMS § 105 lg 1). TsÜS-is on elektrooniliste allkirjade mõistete kasutus ja elektrooniliste allkirjade tasemete tähtsus haldusmenetluse koha pealt jätkuvalt segadust tekitav. Halduslepingu vorminõuete eelduste täidetavuse osas tuleb hinnata lepingu vastavust järgides tsiviilõigusliku lepinguõiguse põhimõtteid. Tsiviilõiguses endas on jäetud hall ala selles osas, millised elektroonilise allkirja tüübid täidavad TsÜS § 80 lõikes 3 sätestatud tingimused. Töö eesmärk oli välja selgitada, kas

plokiahelal põhinev elektrooniline allkiri vastab halduslepingule seaduses sätestatud allkirja nõudele ja eIDAS määrusest tulenevatele klassifikatsioonidele.

Magistritöö esimeses peatükis mõtestati lahti hajussüsteemi mõiste ja nende kasutus. Esimeses selgitatakse hajusraamatutehnoloogiat sellel põhineva plokiahela mõisteid, tehnoloogia kasutust ja tüüpe. Autor mõtestas lahti hajusraamatutehnoloogia mõisteid ja kasutust. Samuti kirjeldas plokiahela tehnoloogiat ja sellega kaasa tulnud nutilepinguid. Autor selgitas eIDAS määruse põhimõtteid ja selle kohaldavust Eestis. Autor osutas, et eIDAS määrus on tehnoloogia neutraalsuse põhimõttest olenemata siiski piirav hajussüsteemide kasutamisest kvalifitseeritud e-allkirjadena. Magistritöö kirjutamise ajal on käimas muudatus uueks eIDAS 2.0 määruse verisoonis vastuvõtmiseks. Küll aga plaanitava eIDAS 2.0 osas on tulnud vastuoluline areng jätta Euroopa komisjoni esialgsest ettepanekust välja elektrooniliste pearaamatute reguleeritud usaldusteenuse osa. Seega on õhus veel jätkuvalt ebaselgust, mis puudutab hajussüsteemide kasutust Euroopa üleselt.

Teise peatüki eesmärk oli analüüsida täpsemalt nutilepingut olemust ja selle siduvust Eesti õigusega. Autor otsis vastus küsimustele, kas ja kuidas on plokiahela tehnoloogiate kasutamine võimalik halduslepingu kirjaliku vorminõude täitmiseks? Selleks uuriti nutilepingut ja kas see vastab lepingu mõistele õiguslikkus mõttes. Lihtsustatult öeldes on nutileping arvutiprogramm, mis väljendab poolte õiguslikke tagajärgi kaasa toovaid kokkuleppeid arvutikoodidena ja täidab neid tingimusi vastavalt eelduste esinemisel, mis on kas sisestatud kasutaja poolt või saadud mujalt süsteemist. Seaduse sõnastuse järgi peaks poolte tahe olema avaldatud sõnaliselt, kas suuliselt või kirjalikult. Autor jõudis järeldusele, et analoogmaailmas ja elektroonilises keskkonnas edastatud tahteavalduse tegemise ning kättesaamise õiguslikud nõuded ei erine. Elektrooniliselt edastatud tahteavalduse puhul loovad tehnilised vahendid paremad võimalused tahteavalduse kättesaamise kontrolliks. Mistõttu on ka nutilepingutega esitatud tahteavaldused õiguslikkus mõttes sobivad halduslepingu sõlmimiseks. Seega olenemata tehniliselt keerukusest on nutilepingud suutelised vahetama tahtavaldusi, mis toovad kaasa õiguslikke tagajärgi.

Töö kolmas peatükk jätkab nutilepingul põhineva halduslepingu vormi uurimisega. Autor analüüsis, kas nutileping täidab halduslepingule seadusega kehtestatud vorminõudeid. Autor jõudis järeldusele, et nutilepingut on võimalik taasesitada, küll aga halduslepingule on seaduses ettenähtud vähemalt kirjalik vorm, mistõttu ei täidaks nutilepingut kasutav haldusleping seadusest tulenevat nõuet. Nutileping ei täida otseselt kirjaliku lepingu vormi, küll aga TsÜS §

80 lg 1 järgi on võrdsustatav kirjaliku vormiga kui leping kvalifitseerub ka elektroonilise vormi alla. Nutileping kvalifitseerub elektroonilise lepingu alla tingimusel, et sellele antud allkirja tüüp samaväärselt täidab elektroonilise allkirja tüüpi. Analüüsist tulenes, et nutilepingu vormis olev haldusleping vastab seaduses nõutavale elektroonilise lepingu vormile. Seega leidis autor vastuse oma esimesele uurimisküsimusele, et plokiahela tehnoloogial põhinevat nutilepingut saab kasutada halduslepingu puhul ja see vastab seadusest tulenevale elektroonilise leping vormi nõudele. Täitmaks ka allkirjastamise nõuet, tuleks nutilepingule lisada niiöelda hajussüsteemi väline allkirja tüüp, et see vastaks ka eIDAS määruse nõuetele ja seejuures täidaks seaduses nõutava elektroonilise digitaalallkirja tüüpi.

Viimases peatükis analüüsiti vorminõude puhul elektroonilise allkirja olemust ja tehingu tegija identifitseerimise ja allkirjastamise nõuet. Autor analüüsis nutilepingul põhineva halduslepingu allkirja nõudeid ja hindab elektrooniliste allkirjade tasemete erisusi. Peamine tähelepanu oli haldusmenetluses kasutatavate õigusaktide allkirja vorminõuetel, tüüpidel ja klassifikatsioonidel. Eestis tähistab mõiste „digitaalallkiri“ (ehk digiallkiri, digiallkirjastamine jm) ainult sellist allkirjastamist tüüpi, mis on seaduslikult sätestatud ning juriidiliselt võrdne omakäelise allkirjaga. See tähendab, et kasutaja isik ja sertifikaadi väljaandja taust on kontrollitud ning allkirja andmise aeg on täpselt fikseeritud. Lihtsamalt öeldes on tuvastatud, kes allkirja andis, ning kindlustatud, et keegi kolmas ei ole allkirjastatavat dokumenti peale selle allkirjastamist muutnud. EUTS § 24 lg 1 kohaselt loetakse digitaalallkirja e-allkirjaks, mis vastab eIDAS määruse artikli 3 punktis 12 sätestatud kvalifitseeritud e-allkirja nõuetele. Selleks, et haldusleping vastaks elektroonilises vormile, tuleb sellele anda ka elektrooniline allkiri. eIDAS määrus artikkel 6 lg 1 nõuab avalikult sektorilt vähemalt täiustatud või kvalifitseeritud allkirja kasutamist. Elektroonilise allkirja atribuuti ei ole seaduses täpsustatud, kuid autori hinnangul saab see olla elektrooniline allkiri, mis vastab täiustatud allkirja nõuetele. Samas ei ole välistatud, et jõutakse seisukohale, et see peab olema digitaalallkiri. Sellest olenemata eIDAS määrus artikkel 25 lg 1 sätestab, et e-allkirja ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud e-allkirjadele esitatavatele nõuetele. Täiustatud allkirja puudub küll kvalifitseeritud allkirjastamis vahend, kuid täidab allkirjastamise funktsioone nagu isiku seostamine tehingu tegijaga ja dokumendi tõendamine. Seega autori hinnangul ei too nutilepingu vormingus halduslepingule antud täiustatud allkiri kaasa veel lepingu tühisust.

EUTS sätestab nõudeid kvalifitseeritud allkirjale, aga ei kõnele elektrooniliselt allkirjast laiemalt. eIDAS määruse artikkel 26 nõuded täiustatud e-allkirjale on järgmised: see on seotud ainuüksi allkirja andjaga; selle abil on võimalk allkirja andja tuvastada; see on allkirjastatud andmetega seotud sellisel viisil, et kõik hilisemad andmete muudatused on tuvastatud. Täiendavalt on nõutud ka see, et see antakse e-allkirja andmiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures kasutada üksnes allkirja andja. Järelikult halduslepingule antav elektrooniline allkiri vastab eIDAS artiklile 26 ehk täiustatud e-allkirjale, siis saab eeldada ka TsÜS § 80 lg 3 nõude täidetavust. Eelnevast võib järeldada, et kuna HMS kõneleb ainult digitaalallkirjast, kui kvalifitseeritud elektroonilisest allkirjast, siis ei ole muud elektroonilised allkirjad mõeldavad. Jällegi annab HMS 7. peatükk mitmeid sätteid, mille puhul tuleb halduslepingule kohaldada tsiviilõiguslikke sätteid, mis võimaldavad lähtuvalt TsÜS § 80 lg-st 3 kasutada elektroonilist allkirja. Seejuures ei ole seatud kohustuseks kasutada digitaalallkirja, vaid nähtud seda kui võimalusena. Autor on seisukohal, et kui antav elektrooniline allkiri täidab kõiki eeldusi, mis on ette nähtud HMS § 55 lg-s 4, vabastamaks dokumendile digitaalallkirja andmisest, siis sobib ka täiustatud e-allkiri eIDAS määruse mõistes. Olenemata sellest saab jõuda siiski järelduseni, et nutilepingu vormis olev halduslepingu täidab seaduses sätestatud vorminõudeid, kui sellele antakse kvalifitseeritud elektrooniline allkiri ehk digitaalallkiri. Tehnoloogia pakub võimalust kasutada nutilepingu vormi, aga sellele peab lisanduma plokiahela väline täiustatud elektrooniline allkiri.

Teiseks uurimisküsimuseks oli, millisele tasemele vastab nutilepinguga antav elektrooniline allkiri ja kas see täidab halduslepingule sätestatud allkirja nõuet? Analüüsi tulemusel jõudis autor järelduseni, et plokiahela tehnoloogia tehnilisest küljest täidab kõiki eIDAS määruse ja Eesti seadustes määratletud halduslepingu vormi nõudeid. Autori leidis, et hajussüsteemil loodavat allkirja saab lugeda elektrooniliseks allkirjaks ja selle nõue täidetuks. Küll aga tegemist ei ole kvalifitseeritud allkirjaga EUTS § 24 lg 1 ega eIDAS määruse artikkel 3 p-i 12 mõistes. Mistõttu seadusest tulenevad vorminõuded, mis nõuavad allkirjastamist, ei ole täidetavad nutilepingutega. Plokiahelal olevad nutilepingud ei vasta seadusest tulenevatele allkirja nõuetele. Selleks peab ennem Euroopas andma plokiahelate krüptovõtmetele vastava standardi, et need hakkaksid kvalifitseeruma elektrooniliste allkirjadena. Siiski allkirjast ainuüksi ei piisa ja nutileping peab jätkuvalt täitma ka teisi lepingu vormi tingimusi. Plokiahelal olevat krüptovõtmete kasutamist on võimalik võrdsustada digitaalse allkirjaga. Plokiahelale või sarnast tehnoloogiat kasutaval platvormile üles laetu nutileping on võrreldav kirjaliku lepingu vormiga allkirjastatusse mõttes. Vastavalt eIDAS määrus artikkel 3 p-le 23 peavad kvalifitseeritud e-allkirja andmise vahendid vastama eIDAS määruse lisas II sätestatud

nõuetele. Nutileping on võimeline täitma kõiki eelnevaid nõudeid, kuid probleem ilmneb lõike 3 osas. Lisa lõike 3 järgi e-allkirja andmiseks vajalikke andmeid võib allkirja andja nimel luua või hallata üksnes kvalifitseeritud usaldusteenuse osutaja. Tegemist on ühe peamise takistusega võrdsustamaks nutilepingute kürptograafiliste võtmete kasutamist kvalifitseeritud allkirja tüübiga. See on peamine puudus, miks hajussüsteemil põhinev nutileping ei täida kvalifitseeritud allkirja nõudeid, sest tal puudub usaldusteenuse osutaja. Vastavaid võtmeid luuakse nutilepingu protokollis endas. Seega vastus teisele uurimisküsimusele on, et nutilepinguga antav allkiri vastab eIDAS määrusest tulenevalt täiustatud allkirja nõudele, kuid ei täida kvalifitseeritud ehk Eesti mõistes digitaalallkirja nõuet. Hajussüsteemidel põhinevate allkirjade kasutuse osas jõudis autor järeldusele, et nutilepingus kasutav detsentraliseeritud identifikaator on palju rohkem identiteedi ja juurdepääsu haldamise kontseptsioon, kus ühelt poolt otsustab identiteedi omanik, kellele ta millise osa oma identiteediinfost annab, ja teisest küljest ei pea andma kõigil juhtudel täielikku identiteediinfot, vaid ainult vajaliku osa. Turvaline digitaalne isikutuvastus ja (kvalifitseeritud) usaldusteenuse olemasolu on ühed peamised nõuded, lubamaks hajussüsteemidel põhinevat allkirjastamist. Praktikas peaks neid detsentraliseeritud identifikaatorid kasutama koos isikut tõendava teabega, mis muudab lihtsamaks digitaalse info vahendamise kolmandate osapooltega.

Autor püstitas uurimistöö hüpoteesiks, et nutilepingutel põhinev haldusleping vastab lepinguõiguse põhimõtetele, aga haldusmenetluses allkirjastamist reguleerivate õigusnormide sõnastused on aegunud ja puudub selgus e-allkirjade kvalifitseerimistaseme õiguslikest tagajärgedest. Magistritöös on jõutud järelduseni, et autori hüpotees pidas paika. Haldusleping vastab TsÜS § 80 järgi elektroonilisele lepingu vormile. Halduslepingu puhul on seadus ettenäinud küll kirjaliku vorminõude, millest tulenevalt nõutakse omakäelisega võrdset allkirja ehk kvalifitseeritud allkirja nõuet täitvat digitaalallkirja. Seega halduslepingust kui sooritavast haldusest, saaksid autori hinnangul lepingu pooled vabalt leppida kokku ka madalama taseme allkirja kasutamises. Vastupidiselt avalikule sektorile saab erasektor ise otsustada, kas ja millise turvalisuse tasemega e-allkirju aktsepteerida. Oluline on siiski teadmine, kes on allkirjastaja tegelik isik. Nagu magistritöös eelnevalt on välja toodud, siis identifitseerimisfunktsiooni saab täita plokiahela väliselt, kasutades selleks hajussüsteemi teenusepakkuja autentimist või krüptovarade puhul sarnase rahakotiteenuse pakkuja autentimist.

Töö analüüsist ja järeldustest võib olla kasu avalikus sektoris plokiahelal põhinevate tehnoloogiliste lahenduste mõistmisel ja nende kasutamisel. Loodetavasti käesolev töö soodustab arutelu hajussüsteemide kasutuse õiguslikest võimalustest avalikus sektoris.

Administrative contract using blockchain technology in a smart contract and its compliance with formal requirements (*Abstract)*

The advent of the eIDAS regulation has increased the interest of service providers offering identification in new technologies, e.g. decentralized system and blockchain. The wider use of blockchain technology has led to automated transactions using solutions known as smart contracts. A more general description of a smart contract is software that executes agreements that uses technological solutions based on a distributed system. The use of a smart contract can also be considered as a container to which a part describing the content of the transaction is added, but whose form and signing requirements are fulfilled by the container itself. In the case of blockchain-based smart contracts, the question arises whether these contracts can be treated as contracts in the sense of Estonian laws and whether confirming a transaction with a cryptographic key is equivalent to a digital signature used in Estonia, if the form of the transaction is determined by law?

The main goal of the master's thesis was to analyze the compliance of a smart contract using blockchain technology with the formal requirements on the example of an administrative contract and including to find the possibilities of using the electronic signature level based on distributed ledger technology based on the current administrative procedure law. In addition, even though according to the principle of contract law, the form of the contract is free, it is unknown whether smart contracts fulfill the criteria of a traditional contract in current law. In Estonia, the suitability of smart contracts according to national law is largely unanalysed, and there is still little literature on this topic in Estonian. Therefore, there is a need to study the scope of the current regulation and the possibilities of interpreting them as contracts. The author analyzed whether blockchain-based smart contracts can be treated as contracts in the sense of Estonian laws and whether confirming a transaction with a cryptographic key is equivalent to a digital signature used in Estonia, if the form of the transaction is legal? The focus of the work was public sector, where there are statutory formal requirements for administrative act forms, including the requirement for a signature. The author mainly bases his analysis on the formal and legitimate assumptions of the administrative contract. According to the Administrative Procedure Act (hereinafter APC) § 99(3) the administrative contract is concluded in writing. In administrative law, in the case of administrative contracts, according to the case, the fulfilment of the form of the administrative contract must be evaluated according to the procedure prescribed for the entry into force of civil law contracts, considering the differences established by the APC (APC § 105 (1)). In GPCCA, the use of the concepts of electronic signatures and

the importance of their levels continue to cause confusion in the example of the administrative procedure. Regarding the enforceability of the formal requirements of the administrative contract, the conformity of the contract must be assessed by following the principles of civil contract law. In the contract law itself, a grey area has been left in terms of which types of electronic signature fulfill the conditions set forth in Section 80(3) of the General Part of the Civil Code Act (GPCCA). The aim was to find out whether the electronic signature based on the blockchain meets the legal signature requirement for the administrative contract and the qualifications arising from the eIDAS regulation.

In the first chapter of the master's thesis, the concept of distributed systems and their use were explained. The first one explains the concept of distributed ledger technology, the blockchain based on it, the use and types of the technology. The author explained the concepts and use of distributed ledger technology. Also described blockchain technology and the smart contracts that came with it. The author explained the principles of the eIDAS regulation and its applicability in Estonia. The author pointed out that eIDAS, regardless of the technology neutrality principle, still restricts the use of distributed systems as qualified e-signatures. At the time of writing the master's thesis, the change to the new eIDAS 2.0 version is underway. Regarding the planned eIDAS 2.0, there has been a controversial development to initially exclude the part of the regulated trust service of electronic ledgers from the proposal of the European Commission. Therefore, there is still uncertainty in the air regarding the use of distributed systems throughout Europe.

The purpose of the second chapter was to analyse more precisely the nature of the smart contract and its bindingness with Estonian law. The author sought answers to questions such as what a smart contract is and whether it meets the concept of a contract in terms of legality. Simply put, a smart contract is a computer program that expresses the agreements of the parties with legal consequences as computer codes and fulfills these conditions according to the presence of prerequisites, which are either entered by the user or received from elsewhere in the system. According to the wording of the law, the will should be expressed verbally, either orally or in writing. The author concluded that the legal requirements for making and receiving a declaration of intent transmitted in the analog world and in the electronic environment do not differ. In the case of an electronically transmitted declaration of intent, technical means create better opportunities for checking the receipt of the declaration of intent. Which is why, in terms of legality, declarations of intent submitted with smart contracts are also suitable for concluding

an administrative contract. Therefore, regardless of technical complexity, smart contracts can exchange statements of will that lead to legal consequences.

In the third chapter of the paper, the analysis of the management contract based on the smart contract was continued, but the form of the contract is emphasized. The author analysed whether the smart contract fulfills the formal requirements established by law for administrative contracts. The author concluded that it is possible to reproduce a smart contract, but the law requires at least a written form for an administrative contract, so an administrative contract using a smart contract would not fulfill the legal requirement. A smart contract does not directly fulfill the form of a written contract, but according to GPCCA § 80 (1) it can be equated with a written form if the contract also qualifies as an electronic form. A smart contract qualifies as an electronic contract provided that the type of signature given to it equally fulfills the type of electronic signature form. The analysis showed that the administrative contract in the form of a smart contract corresponds to the electronic contract form required by law. To also fulfill the signing requirement, an external signature type should be added to the smart contract, so that it also meets the requirements of eIDAS and, at the same time, fulfills the electronic form type digital signature required by law.

In the last chapter, the nature of the electronic signature and the requirement to identify and sign the person making the transaction were analyzed in the case of the form requirement. The author analyzed the requirements for the signature of an administrative contract based on a smart contract and evaluates the differences in the levels of electronic signatures. The focus was on the form requirements, types and qualifications of the signature of legal acts used in the administrative procedure. In Estonia, the term "digital signature" (i.e. digital signature, digital signature, etc.) refers only to a type of signing that is legally valid and legally equal to a handwritten signature. This means that the identity of the user and the background of the certificate issuer have been verified, and the time of signing is precisely fixed. Simply put, it has been identified who signed, and it is ensured that no third party has changed the document to be signed after it has been signed. According to § 24 (1) of the Electronic Identification and Trust Services for Electronic Transactions Act (EITETA), a digital signature is considered an e-signature that meets the requirements of a qualified e-signature set forth in Article 3 (12) of the eIDAS Regulation. The EUTS stipulates the requirements for a qualified signature but does not talk about electronic signatures more broadly. For the administrative contract to correspond to the electronic form, an electronic signature must also be given. The electronic signature

attribute is not specified, but according to the author, it should be a digital signature. However, it is not ruled out that it must be a digital signature.

The requirements of Article 26 of eIDAS for an advanced e-signature are as follows: it is related only to the signatory; it makes it possible to identify the signer; it is associated with the signed data in such a way that all subsequent changes to the data are detected. In addition, it is also required that it is given using the data required for e-signature, which can only be used by the signer at a high level of secrecy. Therefore, the eIDAS requirements are stricter than in the first sentence of § 80 (3) of the GPCCA. Consequently, if the electronic signature given to the administrative contract complies with Article 26 of eIDAS, i.e., the advanced e-signature, then it can also be assumed that the requirement of § 80(3) of the GPCCA is fulfilled. From the above, it can be assumed that since APC only talks about a digital signature as a qualified electronic signature, other electronic signatures are not conceivable. Again, Chapter 7 of the APC provides several provisions in which civil law provisions must be applied to the administrative contract, which allow the use of an electronic signature based on § 80(3) of the GPCCA. At the same time, it is not an obligation to use a digital signature, but it is seen as a possibility. The author is of the opinion that if the given electronic signature fulfills all the requirements stipulated in § 55 (4) of the APC to exempt the document from being signed, then an improved e-signature in the sense of eIDAS is also suitable. Regardless of this, it can still be concluded that an administrative contract in the form of a smart contract fulfills the formal requirements set forth in the law if it is given a qualified electronic signature, i.e., a digital signature. The technology offers the possibility to use the form of a smart contract, but it must be accompanied by an external signature of the blockchain.

Based on the results of the analysis, the author concluded that blockchain technology fulfills all eIDAS and administrative contract forms defined by Estonian laws from a technical point of view. The author found that a signature created on a distributed system can be considered an electronic signature and fulfills this requirement. Dealing with a village is not a qualified signature within the meaning of EITETA § 24(1) or eIDAS Article 3(12). Because the legal formalities requiring signatures are not related to smart contracts. Smart contracts on the blockchain are not equivalent to legal signatures. For this, a corresponding standard must first be given in Europe to the cryptographic keys of blockchains, so that they start to qualify as electronic signatures. But everything alone is not enough, and a smart contract must fulfill other conditions of the form to be the right contract. Cryptographic keys on a blockchain are the potential equivalent of a digital signature. A smart contract uploaded to a blockchain or similar

technology platform is comparable to a written form of contract in terms of the contract. According to Article 3 p. 23 of eIDAS, qualified e-signature means must meet the requirements set out in Annex II of eIDAS. A smart contract can fulfil all the requirements, but the problem appears in paragraph 3. According to section 3 of the Appendix, the data required for e-signature can be created or managed by a qualified trust service provider on behalf of the signatory. This is one of the main obstacles to equate smart contract cryptographic keys with a qualified signature type. This is the main drawback, why a smart contract based on a distributed system does not qualify all the requirements of the letter, because it does not have a trust service provider. The corresponding keys are created in the smart contract protocol itself.

The author hypothesized that an administrative contract based on smart contracts complies with the principles of contract law, but the wording of the legal regulations governing signing in administrative proceedings is outdated and there is no clarity on the legal consequences of the qualification level of e-signatures. The master's thesis has reached the conclusion that the author's hypothesis was correct. The management contract corresponds to the electronic contract form according to § 80 of the GPCCA. In the case of the management contract, although the law provides for a written form requirement, as a result of which a signature equal to a handwritten one, i.e. a digital signature that meets the requirement of a qualified signature, is required, then due to the management contract as the administration to be performed, according to the author, the parties to the contract could freely agree on the use of a lower-level signature as well. In contrast to the public sector, the private sector can decide for itself whether and with which level of security to accept e-signatures. However, it is important to know who this person really is. As previously stated in the master's thesis, the identification function can be performed outside the blockchain, using the authentication of a distributed system provider or, in the case of crypto assets, the authentication of a similar wallet service provider.

The analysis and conclusions of the work can be useful in the understanding and use of blockchain-based technological solutions in the public sector based on the current law. It is hoped that this work will contribute to the discussion about the possibilities of using distributed systems in the public sector.

KASUTATUD ALLIKAD

Kasutatud kirjandus

1. Aedmaa, A., Lopman, E., Parrest, N., Pilving I., Vene E. Haldusmenetluse käsiraamat. – Tallinn. Tartu Ülikooli Kirjastus 2004.
2. Aouidef Y., A., Federico A., Bruno D. Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects. – Frontiers in Blockchain, 2021. https://www.frontiersin.org/article/10.3389/fbloc.2021.564551, (24.04.2023).
3. Bank for International Settlements. Permissioned distributed ledgers and the governance of money. – BIS Working Papers No 924, Jaanuar 2021, lk 2.
4. Busch, C. eIDAS 2.0: Digital Identity Services in The Platfrom Economy. – CERRE Issue paper,10/2022.
5. Brownsword, R. Regulatory Fitness: Fintech, Funny Money, and Smart Contracts. – European Business Organization Law Review, 2019, lk 5 – 27.
6. de Caria R. Blockchain and Smart Contracts: Legal Issues and Regulatory Responses Between Public and Private Economic Law. – Corporate and Financial Markets Law, 2020 (1).
7. de Caria R. Definitions of Smart Contracts: Between Law and Code. – DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law – The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press 2020, lk 19 – 36.
8. Domingo, I. A. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market. – SSI eIDAS Legal Report. European Commission, 2020.
9. Eenmaa, H., Schmidt-Kessen, M. J. Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts. – Computer Law & Secuity Review, 2019/35, lk 69 – 88.
10. Eenmaa, H. Schmidt-Kessen, M. Regulation through code as a safeguard for implementing smart contracts in no-trust environments. – EUI Working Paper LAW, Itaalia, 2017/13.
11. European Law Institute. ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection. – Report of the Euripean Law Institute, 16 Feburary 2023.
12. Gatteschi, V. Lamberti, F., Demartini C. Technologu of Smart Contracts. – DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law – The Cambridge

Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press 2020, lk 37 – 58.

13. Ginter, C., Parrest, N., Simovart M.A. Kontsessiooni vastuoluline regulatsioon Eesti õiguses. – Juridica IV/2012, lk 284-294.
14. Idelberger, F. Merging traditional contracts (or law) and (smart) e-contracts – a novel approach. Arvutivõrgus: https://lawgorithm.com.br/wp-content/uploads/2020/09/MLR2020-Florian-Idelberger.pdf (25.04.2022).
15. Kask, L. E-Eestist e-Euroopasse: elektrooniline allkiri riigisiseses ja piiriüleses suhtluses. – Juridica 10/2017.
16. Kask, L., Laanest, K. Elektroonilise allkirjastamise aja tuvastamine. – Juridica 4/2020, lk 294-304.
17. Madise, Ü. PSK § 26/2. – Eesti Vabariigi põhiseadus. Komm vlj. 5. vlj. Tallinn: Juura 2020, § 19 komm p 1-3.2.
18. Möslein, F. Conflicts of Laws and Codes: Defining the Boundaries of Digital Jurisdictions“. – Universität Marburg, 2018. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3174823 (20.04.2022).
19. Nguyên, Y. Artificial Intelligence Contract: How Algorithms and Machines have Disrupted the way Law is Practices. – PM World Journal, 2019/8 (9).
20. Rosentau, M. Digitaalsed õigusvormid ja IT-lepingu kohustuslik vorm. – (käsikiri autori valduses).
21. Rosentau, M. Arvutivõrgu abil sõlmitud leping kui lepingu erivorm. – Juridica 10/2021.
22. Rosentau, M. Intellektuaalse omandi õigused infotehnoloogias IT autorilepingute kohustuslikud vormid ja vormiga fikseeritav sisu. – Juridica, 2020/5.
23. Scholz, L. Algorithmic Contracts and Consumer Privacy. – Dimatteo L., Cannarsa M., Poncibo C. The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. – Cambridge University Press 2020.
24. Sein, K. Lepingu vorminõuded ja nende järgimata jätmise tagajärjed. – Juridica 2010/7.
25. Simovart, M. A., Parind, Mart. Riigihangete seadus. Kommenteeritud väljaanne. Juura, Tallinn 2019.
26. Sorge, C., Leicht, M. Blockchain-based electronic time stamps and the eIDAS regulation: The best of both world. – Scrpited, Volume 19, Issue 1, Feburary 2022.
27. Tai, E. Challenges of Smart Contracts. Implementing Excuses. – DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law – The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press 2020.

28. Tai, E. Formalizing contract law for smart contracts. – Tilburg Private Law Working Paper Series, 2017 (6).
29. Tshibende, L.-D. M. Smart Contracts: Issues of Property and Secuirty Rights. – DiMatteo, L., Cannarsa, M., Poncibo, C. Smart Contracts and Contract Law – The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press 2020, lk 240 – 250.
30. Varul, P., jt (koost). Võlaõigusseadus I. Üldosa (§§ 1 – 207). Komm. vlj. 2. tr. Tallinn: Juura 2016.
31. Varul, P., jt (koost). Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne. Juura, Tallinn 2010.
32. Varul, P. Tahteavaldus ja selle tegemine. – Juridica 2010/7, lk 497 – 507.
33. Veerpalu, A. Regulatory challenges to the use of distributed ledger technology: analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence. – Doktoritöö. Juhendaja Martin Ebers, Anna-Maria Osul. Tartu: Tartu Ülikooli Kirjastuse trükikoda.
34. Veerpalu, A. jt. The hybrid smart-contract agreement challenge to European electronic signature regulation". – International Journal of Law and Information Technology. Oxford University Press, 2020/28 (1), lk 39 – 84.
35. Woebbeking, M. K. The Impact of Smart Contracts on Traditional Concepts of Contract Law. – Journal of Intellectual Property, Information Technology and E-Commerce Law, 2019/10.

Kasutatud normatiivaktid

1. Art 8-ter(2) DL 135/2018 of 14 December 2018, converted into law by Law 12/2019 of 11 February 2019.
2. E-identimise ja e-tehingute usaldusteenuste seadus. – RT I, 03.03.2023, 3.
3. 23. juuli 2014. aasta Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. – ELT L 257/73.
4. Haldusmenetluse seadus. – RT I 13.03.2019, 55.
5. Halduskohtumenetluse seadustik. – RT I, 11.03.2023, 21.
6. Provision 44-7061 A, Arizona Bill HB 2417/2017. Arvutivõrgus: https://legiscan.com/AZ/text/HB2417/id/1497439, (19.04.2023).
7. Põhiseadus. – RT I, 15.05.2015, 2.
8. Riigihangete seadus. – RT I, 23.02.2023, 7.

9. Tsiviilseadustiku üldosa seadus. – RT I, 20.06.2022, 33.
10. Võlaõigusseadus. – RT I, 17.03.2023, 80.

Kasutatud kohtupraktika

1. RKHKo nr 3-13-481
2. RKHKo nr 3-3-1-64-03
3. RKTKo nr 3-2-1-49-04
4. RKHKo nr 3-3-1-25-14
5. RKTKo nr 2-15-15662/55
6. RKHKo nr 3-3-1-71-05

Muud kasutatud allikad

1. Decentralized Identifiers (DIDs). Arvutivõrgus: https://w3c.github.io/did-core/ (19.03.2023).
2. DSS Demonstration WebAPP. Arvutivõrgus: https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation 17.03.2023.
3. DocuSign veebileht. Arvutivõrgus: https://www.docusign.com/ (19.04.2023).
4. E-Estonia. Arvutivõrgus: https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf (12.01.2023).
5. 23. juuli 2014 Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. – ELT L 257, lk 73-114.
6. European Digital SME Alliance. Digital SME pleads for blockchain as a security tool for EU Digital Identity. Arvutivõrgus: https://www.digitalsme.eu/digital-sme-pleads-for-blockchain-as-a-security-tool-for-eu-digital-identity/ (21.03.2023).
7. Euroopa Komisjoni ettepanek millega muudetakse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (eIDAS), seletuskiri. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281 (23.04.2023).
8. European Central Bank (ECB). Virtual Currency Schemes – A Further Analysis. Veebruar 2015. Arvutivõrgus: www.ecb.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, (11.03.2023), lk 33.
9. Erlich, M. Riigi Infosüsteemide Amet. E-Allkirjad Euroopas ja nende käsitlemine Eestis. Arvutivõrgus: https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/usaldusteenused-ja-koostoo (12.03.2023).

10. European Parliamentary Research Service. Markets in crypto-assets (MiCA), november 2022. Arvutivõrgus: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI(2022)739221_EN.pdf (10.01.2023).
11. IBM. What are smart contracts on blockchain? Arvutivõrgus: https://www.ibm.com/topics/smart-contracts (15.04.2023).
12. ID. Digitaalne allkirjastamine ja elektroonilised allkirjad. Arvutivõrgus: https://www.id.ee/artikkel/digitaalne-allkirjastamine-ja-elektroonilised-allkirjad/ (5.04.2023).
13. International Association for Trusted Blockchain Association internationale sans but lucratif. Open Letter for the preservation of the Electronic Ledger's provisions in eIDAS 2. 13. märts 2023. Arvutivõrgus: https://inatba.org/news/savesection11-eidas2-trusted-electronic-ledgers-open-letter/ (23.03.2023).
14. Komisjoni rakendusmäärus (EL) 2015/1502. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32015R1502 (21.03.2023).
15. Komisjoni rakendusotsus (EL) 2015/1506. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32015D1506 (19.03.2023).
16. Kirova, M. Overview of pre-notified and notified eID schemes under eIDAS. Arvutivõrgus: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS (19.03.2023).
17. Koalitionsvertrag zwischen CDU, CSU und SPD (coalition agreement, 14 March 2018), p. 70 et seq. Arvutivõrgus: https://www.bundesregierung.de/Content/DE/StatischeSeiten/Breg/koalitionsvertrag-inhaltsverzeichnis.html, (21.04.2023).
18. Law Commission. Smart legal contracts. Advice to Government. Presented to Parliament by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty. November 2021. Arvutivõrgus: https://www.lawcom.gov.uk/project/smart-contracts/ (10.04.2023).
19. PandaDoc veebileht. Arvutivõrgus: https://www.pandadoc.com/electronic-signature-software/?utm_source=google&utm_medium=cpc&utm_campaign=Google_Search_NB_Competitor_EU&utm_content=DocuSign&utm_device=c&utm_placement=&utm_term=docusign&utm_creative=613599673654&gclid=Cj0KCQjwlumhBhClARIsABO6p-wL34m1WkUzq09peOubWHCgegqiTcZh-JMvsFZMTYNDsqqguTo1lJcaAj3DEALw_wcB (19.04.2023).

20. Pollet, M. Blockchain might be the solution to the digital identity hurdle. – EURACTIV France. Arvutivõrgus: https://www.euractiv.com/section/digital/news/blockchain-might-be-the-solution-to-the-digital-identity-hurdle/ (21.11.2022).
21. Riigi Infosüsteemi Amet. Usaldusteenused ja koostöö. Arvutivõrgus: https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/usaldusteenused-ja-koostoo (19.03.2023).
22. Riigi Infosüsteemide Amet. E-identimise skeemid. Arvutivõrgus: https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/usaldusteenused-ja-koostoo (19.03.2023).
23. Riigi Infosüsteemi Amet. Dokumendivahetuskiht DHX. Arvutivõrgus: https://www.ria.ee/et/riigi-infosusteem/dokumendivahetuskiht-dhx.html (24.05.2022).
24. Registrite ja infosüsteemide keskus (RIK). RIK lõi ühenduse Euroopa Liidu kaubamärkide plokiahela võrguga. Arvutivõrgus: https://www.rik.ee/et/news/rik-loi-uhenduse-euroopa-liidu-kaubamarkide-plokiahela-vorguga (19.04.2023).
25. Secure Sockets Layer (SSL). Arvutivõrgus: https://www.ssl.com/et/KKK/faq-digitaalallkirjad-ja-dokumentide-allkirjastamine/ (12.10.2022).
26. Seletuskiri e-identimise ja e-tehingute usaldusteenuste seaduse eelnõu juurde, 237 SE, lk 17–18. https://eelnoud.valitsus.ee/main#wmHbSe8s (19.04.2023).
27. S. Bian jt. IcoRating: A Deep-Learning Syster for Scam ICO Identification. 08.03.2018. Arvutivõrgus: https://arxiv.org/pdf/1803.03670.pdf, (27.03.2023).
28. SK ID Solutions AS koduleht. Arvutivõrgus: https://www.skidsolutions.eu/ettevottest/ (20.04.2023).