TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse instituut

Hettel Varik

E-identiteet Eesti ja Euroopa Liidu õigusruumis: Euroopa Parlamendi ja Nõukogu e-identimise ja e-tehingute jaoks vajalike usaldusteenuste määruse kohaldamine Eestis – kujunemislugu, probleemid ja eelseisvad väljakutsed

Magistritöö

Juhendaja: *M.A.* Jaana Sahk
Kaasjuhendaja: *dr.iur*. Carri Ginter

Tallinn 2015

SISUKORD

SISSEJUHATUS

Käesolev magistritöö on analüüs e-identiteedi kujunemisest nii Eesti kui Euroopa Liidu õigusruumis, Euroopa Parlamendi ja nõukogu e-identimise ja e-tehingute jaoks vajalike usaldusteenuste määruse kohaldamisest Eestis e-identiteedi vallas ja sellega kaasnevatest probleemidest ning eelseisvatest väljakutsetest. Viidatud määrus käsitleb lisaks e-identimise regulatsioonile ka usaldusteenuste ja e-dokumentide regulatsiooni, kuid käesolev magistritöö keskendub ennekõike määruse e-identimise osale, s.o on määruse peatükk II, ja puudutab teisi osi üksnes juhul, kui need on vääramatult seotud e-identimisega (nt ajaloolises protsessis, kus digitaalallkirja käibele tulek on oluline teetähis tulevase eID välja kujunemisel). Käesolevas töös on käsitletud nii e-identiteedi tekkimise ajalugu ja asjaolusid, e-identiteedi tunnuseid ning uut õiguskorda alates 2014. aastal vastuvõetud EL 910/2014 määrusest (edaspidi ka eIDAS määrus).

Käesoleva magistritöö esimeses peatükis selgitab autor töös käsitletavaid mõisteid ning annab ülevaate, milline oli õiguslik olukord Eestis ja Euroopa Liidus enne töö teises osas käsitletava eIDAS määruse vastuvõtmist. Ajaloolist kujunemist käsitlev osa on oluline mõistmaks, miks uut regulatsiooni vaja oli. Samas on see oluliseks aluseks nimetatud määruse õiguslikule sisule, sest eIDASt ei töötatud välja teoreetilistest mõttekäikudest lähtuvalt, vaid praktilistest vajadustest tulenevalt ning olukorda reguleerivat õiguslikku külge järejpidevalt edasi arendades.

Autori peaülesandeks on käesoleva töö teises osas läbi analüüsi jõuda selguseni, kuidas eIDAS määrust e-identimise küsimustes Eestis kohaldada – kas Eestis kasutusel olevad e-identimise vahendid kvalifitseeruvad ning millisel tasemel kvalifitseeruvad viidatud Euroopa Parlamendi ja nõukogu määruse kohastesse e-identimise süsteemide (i.k *electronic identification scheme*) kategooriatesse, millised on sellega kaasnevad väljakutsed ja võimalikud probleemkohad. Samuti analüüsitakse uusi menetlusprotsesse, mis käesoleva määruse ning selle alusel vastu võetud või vastuvõtu eel rakendusaktide kohaselt antud protsessis kohalduvad. Käesolevas töös on kasutatud e-identimise süsteemide kategoriseerimisel ja nende usaldusväärsuse tasemete määramise analüüsil EL 910/2014 määruse artikkel 8 lõike 3 alusel vastu võetava ning hetkel eIDAS ekspertgrupis arutluse all oleva Euroopa Komisjoni rakendusotsuse 08.04.2015 eelnõud, mis võib viimaste ekspertidega peetavate arutelude käigus täpsustuda, kuid mille raames on läbi analüüsi püütud illustreerida

Eestis väljaantavate erinevate e-identimise vahendite erinevaid väljakutseid üleeuroopalises tunnustamisskeemis. Antud rakendusotsus on kavandatud komitees hääletamisele jõudma 2015 I poolaasta jooksul. Piiratud ligipääsuga eelnõu on käsoleva töö Lisas nr 1.

Teema valikul lähtus autor töö fookusesse valitud küsimuste ja nendega seonduvate väljakutsete aktuaalsusest, valdkonnas kiirestitoimuvatest arengutest ja arutelu vajalikkusest globaliseeruva digitaalse ühisturu tingimustes. Kuna igapäevaselt tekib juurde järjest uusi internetipõhiseid teenuseid, milleks kasutatakse veebipõhist autentimist, on elektroonilise identiteedi kasutamine enamusele eestlastest juba väga käepärane – ID kodulehe andmetel[1] on 21. aprilli seisuga käesoleval aastal teostatud Eestis 341 975 853 elektroonilist isikutuvastust. Paraku ei ole see nii omane kogu ülejäänud Euroopale. Võimalus tuvastada ennast turvaliselt internetis ID-kaardi või mõne muu e-identimise vahendi abil või anda digiallkirja, on küll olemas ka mitmetes teistes Euroopa Liidu riikides (nt Austria, Soome, Belgia, Hispaania), kuid probleemiks on see, et enamasti liikmesriigid neid vastastikku ei tunnusta ning piiriüleste teenuste puhul käib kõik endistviisi paberil. Teisalt on uus regulatsioon nii värske, et selle sisulised osad on veel rakendumata, mitmed rakendusaktid alles väljatöötamisel ning parimate praktikate vahetamine seismas ees, mistõttu on äärmiselt huvitav analüüsida käesolevas ajahetkes toimuvaid arenguid, mille kujundamisse on veel võimalik ekspertidel oma panus anda; analüüsida ning hinnata, mis vajab eelseisvate ülesannete valguses ettevalmistamist, siseriiklikku reguleerimist, määramist, muutmist ja/või planeerimist. Kuna regulatsioon ise pakub Euroopa Liidu liikmesriikidele võimalust siiski oluliseks koostöö tõhustamiseks ning kaasab eIDAS määruse alusel loodava koostöövõrgu tegevustesse ka Euroopa Majanduspiirkonna riigid, on eelseisvad arengud kahtlemata suure praktilise väärtusega.

Käesolevas töös on:

1. Antud ülevaade:
   - e-identiteedi kujunemisest Eestis ning paralleelarengust Euroopa Liidus;
   - Eestis kasutusel olevatest e-identimise vahenditest;
2. Analüüsitud ja vastatud küsimustele:
   - milline on eIDAS määruse kohaldamisala ning mida tuleb selle kohaldamiseks Eestis e-identimise vallas teha;
   - mis on antud määruse kohaselt e-identimine ning millised on e-identimise süsteemid;
   - kuidas toimub ja mida tuleb arvestada e-identimise süsteemidest teavitamisel;

[1] Vt http://www.id.ee/ (21.04.2015). Andmed 08:04 kellaajalise seisuga.

3. Käsitletud:
    - e-identimise süsteemide usaldusväärsuse tasemete võimalikku määramist;
    - teavitatud süsteemidele kohalduvat koosvõime raamistikku ning vastastikuse hindamise läbiviimisprotsessi;
    - määrusest tulenevaid teisi e-identimisele kohalduvaid põhimõtteid;
4. Hinnatud Eesti e-identimise süsteemide väljavaateid vastastikuseks tunnustamiseks;
5. Pakutud välja lahendused Eestis kasutusel olevate e-identimise süsteemide tunnustamiseks vastavalt eIDAS määrusele.

Uurimuses keskendub autor e-identimise regulatsiooni arengule ja rakendumisele, selgitades e-identimise ühtlustamise vajalikkust Euroopa Liidu majandusruumis ning eraldi käsitledes Eesti osa nimetatud protsessis.

Käesolev magistritöö tugineb rahvusvahelistele uurimustele, Euroopa Liidus läbiviidud strateegilistele analüüsidele, teaduslikele uurimustöödele ja kohalduvatele õigusaktidele. Eeltoodutest olulisemad on vastavalt:

- United Nations E-Government Survey 2014. E-Government for the Future We Want. New York, 2014;
- Feasibility Study on an Electronic Identification, Authentication and Signature Policy (IAS). European Union, 2013;
- EUROPE 2020. A strategy for smart, sustainable and inclusive growth, COM(2010) 2020 final;
- Digital Agenda for Europe, COM(2010)245 final;
- 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;
- Komisjoni rakendusotsus (EL) 2015/296, 24. veebruar 2015, millega kehtestatakse menetluskord liikmesriikidevaheliseks koostööks e-identimise valdkonnas vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 7;
- Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artiklite 8 ja 9 lg 1 alusel antava komisjoni rakendusotsuse eelnõu (töö Lisas 1).

Samuti toetavad käesolevat magistritööd Eestis läbiviidud uuringud, strateegilised dokumendid, arengukavad ja õigusaktid. Eeltoodutest olulisemad on vastavalt:

- E-teenuste kasutamise tulemuslikkus ja mõju. Uuringu aruanne. Tallinn, 2013;
- Eesti Euroopa Liidu poliitika 2011–2015;
- Eesti infoühiskonna arengukava 2020;
- Isikut tõendavate dokumentide seadus; välismaalaste seadus; rahvastikuregistri seadus; isikut tõendavate dokumentide andmekogu pidamise põhimäärus; digitaalse isikutunnistuse vormi, tehnilise kirjelduse ja digitaalsele isikutunnistusele kantavate andmete loetelu kehtestamine; Eesti Vabariigi välja antava elamisloakaardi vormi ja tehnilise kirjelduse ning elamisloakaardile kantavate andmete loetelu kehtestamine ja elamisloakaardile kantavate digitaalsete andmete kehtivusaja määramine.

Käesoleva töö kirjutamisel on autor kasutanud ajaloolist, analüüsiv-võrdlevat- ja sünteesivat meetodit. Ajaloolist aspekti on kasutatud ülevaate andmisel uuritava valdkonna kohta, analüüsiv-võrdlevat uue regulatsiooni sisu käsitlemisel ja sünteesivat järelduste tegemisel.

Töö autor on püstitanud järgmised tööhüpoteesid, mille paikapidavust või paikapidamatust ta oma kirjutises näitab:

1. Vastastikuse tunnustamise vallas: kõigil EL liikmesriikidel, s.h Eestil, tuleb alates eIDAS määruse jõustumisest tunnustada kõiki teiste liikmesriikide e-identimise süsteeme;
2. Teavitamismenetluse vallas: olles teavitav liikmesriik või mitte-teavitav liikmesriik, üks e-identimise vahend võrdub üks e-identimise süsteem;
3. Ettenähtud koostöö vallas: koostööd tuleb teha sõltumata e-identimise süsteemi(de)st teavitamisest ja koostöövõrk tagab riiklike e-identimise süsteemide üleeuroopalise harmoniseerumise.

Seega on magistritöö uurimisaineks e-identimise regulatsioon Eestis ja Euroopa Liidus koos võimaluste otsimisega, kuidas Eestis kasutusel olevad e-identimise vahendid sobivaimal võimalikul viisil kvalifitseerida Euroopa Liidu e-identimise regulatsioonile vastavatesse e-identimise süsteemidesse. Töös on käsitletud ka autori ettepanekud selleks, mil viisil vastavat kvalifitseerimist parimal võimalikul moel saavutada.

Autor tänab oma juhendajat Euroopa Komisjoni lähetatud Eesti rahvuslikku eksperti Jaana Sahk'i ja Tartu Ülikooli määratud kaasjuhendajat Carri Ginter’it, kelle toetusel töö valmis. Samuti avaldab autor tänu Majandus- ja Kommunikatsiooniministeeriumi, Riigi Infosüsteemide Ameti, Siseministeeriumi ja Politsei- ja Piirivalveameti ekspertidele, kellega käesoleva Euroopa Liidu e-identimise regulatsiooni kohaldamisega seotud küsimusi arutati.

I. ELEKTROONILINE IDENTITEET JA E-IDENTIMINE

1.1. Mõiste käsitlus

E-identimise lahtimõtestamiseks tuleb esmalt avada, kust saab alguse ja mis on elektrooniline identiteet. Selleks tuleb alustada identiteedist ja identiteedi samasuse tuvastamisest.

Identiteet on omaduste hulk, mis teeb objekti unikaalseks võrreldes teiste samalaadsete objektidega. Identiteeti saab käsitleda ka kui teadmist endast sotsiaalsetes olukordades ja suhetes[2], näiteks kuulumine teatud kollektiivi, rahvusesse, vähemusgruppi või huvirühma. Tavaliselt on identiteedi teadvustamine vajalik mingit laadi ressursi või hüvede kasutamiseks, milliseks tuleb isik esmalt identifitseerida ehk kellenagi ära tunda, samastada. Seega võib öelda, et isikusamasus on kontrollitud veendumus, et isik on ikka seesama, kellena ta väidab end olevat. Eeltoodust johtuvalt käsitlen käesolevas töös identiteeti, kui isikulist samasust.

Isikusamasust on võimalik kindlaks teha erinevate meetodite ning vahenditega, kuid vajadus erinevate meetodite valimise järele võib olukorrast sõltuvalt suuresti varieeruda. Näiteks kriminoloogias võib isikusamasust tuvastada protsessi läbi, mis seisneb inimese teadvuses või välismaailma jäetud jäljes salvestunud informatsiooni järgi jälje jätnud objekti tunnuste väljaselgitamises ning nende tunnuste võrdlemises selle objekti tunnustega, kes või mis võis antud jälje jätta[3]. Panganduses kehtib nõue tuvastada isik enne esmakordset pangakonto avamist krediidi- või finantseerimisasutuse poolt läbi mitmete põhjalike hoolsusmeetmete[4] kontrollimise – kliendi või tehingus osaleva isiku isikusamasus tuvastatakse esmalt esitatud dokumendi alusel, seejärel kontrollitakse andmed üle usaldusväärsest ja sõltumatust allikast hangitud teabe läbi, tuvastatakse isikute isikusamasus ja kontrollitakse esindusõiguse olemasolu, tuvastatakse tegelik kasusaaja, hangitakse teavet isiku ärisuhete ja tehingu eesmärgi ning olemuse kohta jpm – sh tuleb esmakordne isikusamasuse tuvastus läbi viia isiku või tema esindajaga ka füüsiliselt samas kohas viibides[5]. Olgu isiku samasuse kindlakstegemise protseduur erinevates elulistes situatsioonides kui tahes erinev, läbib neid kolm kriteeriumit, mis peavad olema täidetud – selleks on usaldusväärsus, piisavus ja

[2] Eesti keele seletav sõnaraamat. Arvutivõrgus: http://www.eki.ee/dict/ekss/index.cgi?Q=identiteet&F=M (28.02.2015).
[3] John F. Williams. Trace Evidence. Journal of Criminal Law, Criminology and Police Science. Northwestern University School of Law, 1958. Volume 49, Issue 3, p. 285.
[4] Rahapesu ja terrorismi rahastamise tõkestamise seadus, § 13 jj.
[5] *Ibid*., § 15 lg 1.

võrreldavus. Tuvastamismehhanism peab tagama usaldusväärse tulemuse, mis on piisav antud olukorras isiku määratlemiseks ning on võrreldav teiste samalaadsete tulemustega.

Elektroonilises keskkonnas puudub tavapärane võimalus vahetult kontrollida erinevaid unikaalseid tunnuseid, mille alusel tavapäraselt isikuid eristatakse. Seetõttu on elektrooniline identiteet ja isikusamasuse tagamine tihedalt seotud mõistega autentimine, mille käigus veendutakse isiku vastavuses tema identiteedile. Sarnaselt füüsilise identiteediga saab jagada elektroonilise identiteedi kaheks, nö tõestatud identiteediks või siis väitel põhinevaks, kus kasutaja ligipääs on kaitstud küll kasutajanime ja parooliga, kuid puuduvad välised sertifitseerijad, kes tegelikult kinnitaksid valitud pseudonüümi seost isikulise identiteediga. Tõestatud identiteedi tagamiseks ja toimingutes siduvate digitaalsete jälgede saamiseks, nii et need oleksid ümberlükkamatud, rakendatakse digitaalsete isikusamsuste kontrolli ja isikute tahte elektrooniliste kinnituste kaitseks mitmeid krüpteerimise ning turvatehnoloogiaid. See seob elektroonilise identiteedi tihedalt avaliku võtme taristu, digitaalsete dokumentide ja sertifitseerimise valdkonnaga. Isiku tahte kinnitamine elektroonilises keskkonnas toimub isiku poolt digitaalse allkirja andmisega.

Elektrooniline identiteet (lühendatult ka eID) on isikutuvastusvahend, millega isik saab elektroonilises keskkonnas tõendada, et ta on see, kelleks ennast nimetab ning seeläbi ligipääsu elektroonsetele teenustele. Elektrooniline identiteet on üks ühele seotud selgelt konkreetse füüsilise isikuga[6], seega lubab ka elektrooniline identiteet isikutel end üksteisest eristada. Eesti mõistes on eID elektrooniliseks kasutamiseks mõeldud isikut tõendav dokument, nagu ID-kaart, mobiil-ID, digi-ID, elamisloakaart ja e-residendi digi-ID, mida väljastab Politsei- ja Piirivalveamet.

eID-d on Eestis võimalik kasutada elektroonilise isikutuvastuse vahendina (autentimine veebikeskkondades), digitaalallkirja andmiseks, isikute krüpteeritud andmete edastamiseks või vastuvõtmiseks, elektroonilise võtmena läbipääsusüsteemides ning samuti ka kui kliendikaarti (võimaldades elektrooniliselt lugeda isikuandmeid füüsiliselt kaardilt).

eID puhul kasutatakse Eestis nn turvalist andmekandjat, mis koosneb kiibist, selles talletatud sertifikaadist ja võtmest, mis tagavad tehtavate toimingute turvalisuse. Seejuures on sertifikaat

[6] Gerhard Jakisch. E-signature versus E-Identity: the creation of the digital citizen. Database and Expert Systems Applications. IEEE Xplore Digital Abstract, 2000, p. 316.

isikuga seotud elektrooniline dokument, mis sisaldab isikuandmeid ja tema tuvastamiseks vajalikku võtit[7]. Avaliku võtme krüptograafias kasutatakse tegelikkuses aga kahte võtit[8] – avalikku ja salajast. Salajane võti tuleb hoida salajas ja seda kasutatakse dekrüpteerimiseks või allkirjastamiseks ehk signeerimiseks. Avalikku võtit kasutatakse vastavalt krüpteerimiseks ja vastava salajase võtmega antud signatuuride verifitseerimiseks. Avalik ja salajane võti genereeritakse korraga ja nad on omavahel seotud eelnevalt kirjeldatud omaduste abil, kuid avalik võti ei paljasta informatsiooni salajase võtme kohta ja nii pole võimalik avalikku võtit kurjasti ära kasutada. Et siduda võtmepaar konkreetse isikuga, liidetakse avaliku võtme juurde isikuandmed ning see moodustabki sertifikaadi. Nagu avalik võti, on ka seda sisaldav sertifikaat avalik. Privaatne võti on sellega küll seotud, kuid seda hoitakse salajas. Et sertifikaat oleks sealjuures aga usaldusväärne, peab kolmas tunnustatud osapool (sertifitseerimiskeskus[9]) seda kinnitama. Eestis on selleks kolmandaks tunnustatud osapooleks AS Sertifitseerimiskeskus, kes kinnitab sertifikaadi (isikuandmete ja avaliku võtme seose) allkirjastades selle oma privaatse võtmega.

1.2. Vajadus ühtsete reeglite järele

Riigi Infosüsteemi Ameti andmetel on jaanuari 2014 seisuga Eesti ID-kaart enam kui 91% Eesti elanikkonnast ning mobiil-ID enam kui 30 000 inimesel. Vähemalt 50% ID-kaardi omanikest on kaarti kasutanud elektroonilises keskkonnas autentimiseks ja/või digitaalallkirja andmiseks.[10]

Esindamaks Eesti huve Euroopa Liidus, on meie valitsusel oluline roll määrata avalikkusega konsulteerides kindlaks eesmärgid ja põhimõtted, millele Eesti riik oma Euroopa Liidu suunalises tegevuses toetub. Praegu kehtiv "Eesti Euroopa Liidu poliitika" raamdokument[11] hõlmab aastaid 2011-2015 ning seal sisalduvad Eesti Euroopa Liidu suunalise poliitika raamseisukohad. Prioriteedina tõuseb Eesti seisukohalt esile Euroopa Liidu konkurentsivõime suurendamine ning siseturu arendamine ja selle põhimõtete laiendamine, et luua praeguse killustatud siseturu asemel Euroopa Liidu ühtne turg, kus oleks võimalikult vähe takistavaid

[7] Digitaalallkirja seadus § 5 lg 1.
[8] Xiang-dong Wu, Jian Zhou. E-commerce „identity“ – – a digital certificate. Journal of Chemical and Pharmaceutical Research, 2014. Volume 6, Issue 10, p. 653.
[9] I.k. *certification authority.*
[10] Andmed elektrooniliselt kättesaadavad: https://www.ria.ee/elektrooniline-identiteet/ (14.03.2015).
[11] Arvutivõrgus: https://www.riigikantselei.ee/valitsus/valitsus/et/riigikantselei/euroopa/Eesti%20EL%20poliitika_EST.pdf (26.02.2015).

erisusi teenuste, kaupade ning isikute piiriülesel liikumisel. Eesmärgiks on seega siseturu integratsioon. Selle saavutamiseks nähakse vajadust lihtsustada ettevõtluskeskkonda Euroopas. Ettevõtluskeskkonna lihtsustamiseks on tarvis jõuda Euroopa ühtse lepingu-õiguseni, mis tugineks suures osas elektroonilise suhtluse edendamisele.

Ettevõtluskeskkonna lihtsustamiseks nähakse vajadust 1) luua ühtne euromaksete piirkond, 2) luua ühtne elektrooniliste sisuteenuste turg, 3) tõhustada õiguste kaitset piiriüleste vaidluste korral kodanike ja ettevõtjate jaoks, 4) luua piiriüleste e-hangete süsteem, 5) nüüdisaegse mobiilside kättesaadavuse järele maksimaalses võimalikus ulatuses, 6) laiendada Euroopa Liidu standardiseerimise raamistikku teenusstandarditele, et tagada teenuste piiriülesus, 7) lihtsustada kvalifikatsioonide tunnustamist erinevates liikmesriikides ning 8) tagada kohtulahendite vaba liikumine.[12]

Sellest lähtuvalt kerkibki vajadus üleeuroopaliselt toimiva sidusa ja sujuva elektroonilise suhtluse ning usaldusväärse e-autentimise ja digitaalallkirjade lahenduste kasutatavuse järele.

Kuna majanduskasv ja töökohtade loomine ning siseturu toimimise tõhusus põhineb Eesti seisukohast tänapäeval eelkõige elektroonilisel suhtlusel, siis on Eesti Euroopa Liidu poliitika oluliseks prioriteediks sellise toimiva digitaalse ühtse turu loomine. Praktikas on seda mõistetud ka Euroopa Liidu tasandil ja 1. novembril 2014 ametisse astunud uus Euroopa Komisjon (edaspidi ka komisjon) muutis varasemat esimese ja teise klassi volinike süsteemi asendades selle uue koostöövormiga, kus korraga koordineeritakse mitme voliniku tööd koosseisudes, mis võivad vastavalt vajadusele muutuda – enam keskendutakse valdkondade arendamisele ja mitte ühe kindla portfelli juhtimisele. Uues komisjonis nähti esimest korda ette digitaalse ühtse turu valdkonna arengu eest vastutav asepresidendi ametikoht[13].

Digitaalse ühtse turu poliitika kujundamisel lisandub elektroonilise autentimise ja digitaalallkirjade sisseviimise tehnilisele poolele ilmne vajadus ka üleeuroopalise usalduse kujundamine järele nende suhtes. Usalduse puudumine elektroonilise autentimise ja digitaalallkirjade suhtes riigi ja isiku või isiku ja isiku vahelistes suhetes võibki olla põhjuseks, miks tarbijad, ettevõtjad ja ametiasutused on elektrooniliste tehingute tegemise ja

[12] Eesti Euroopa Liidu poliitika 2011-2015.
[13] Seda juhib käesoleval ajal Eesti endine peaminister Andrus Ansip.

uute teenuste kasutuselevõtu suhtes tagasihoidlikud[14]. Selleks tuleb kõiki elektroonilise suhtluse ja identimise protseduure rakendada ranges vastavuses isikuandmete kaitse põhimõtetega[15]. Arvestada tuleb ka võimaliku küberkuritegevuse ning küberrünnakutega, kuna ka need omavad mõju digitaalse turu usaldusväärsuse tagamisele[16].

Eesti riigi ja Euroopa Liidu ühine huvi – luua turvaline ja takistusteta digitaalne ühtne turg – on võimalik tagada vaid juhul, kui eelpool loetletud seisukohti suudetakse arvestada, ühistes reeglites kokku leppida ja digitaalse keskkonna turvalise kasutamise usaldusväärsus tagada.

E-identimise[17] ja e-autentimise vastastikune tunnustamine on põhitegur, mis loob aluse digitaalse ühisturu toimimiseks. See eeldab kindlat, turvalist ja usaldusväärset e-identimise raamistikku.

1.3. Kujunemise protsess: e-usaldusteenuste kujunemisest kuni e-identiteedini Eestis ja Euroopa Liidus

1.3.1. Algus-aastad – 1990ndad

Eesti e-riigi kontseptsioon loodi 1990. aastate lõpus. See tugineb paljuski riigi infosüsteemide andmevahetuskihile X-tee[18] ja riigi poolt väljaantavatele digitaalsetele isikut tõendavatele dokumentidele.

11. mail 1998. aastal moodustas EV siseminister oma käskkirjaga identifitseerimiskaardi ja selle spetsifikatsiooni väljatöötamise ning väljastamise ettevalmistamise komisjoni[19].

---

[14] Lei Xin-sheng. E-commerce safety technology. 1st edition. National Defence Industry Press. Beijing, 2012, p. 35.

[15] Geraint Price. The benefiits and drawbacks of using electronic identities. Information Security Technical Report. May 2008. Volume 13, Issue 2, p. 97.

[16] Matthew L. Williams. Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. British Journal of Criminology. Published online: http://bjc.oxfordjournals.org/content/early/2015/04/27/bjc.azv011.full.pdf+html?sid=5601ffe5-8aec-45c8-b12f-06c32f1fca5f, April 27, 2015, p. 1-28.

[17] Elektoonilises keskkonnas *identimise* mõiste on võetud kasutusele eIDAS määruses, mille kohaselt on e-identimine protsess, mille käigus kasutatakse elektroonilisi isikutuvastusandmeid, mis tähistavad üheselt füüsilist või juriidilist isikut või juriidilist isikut esindavat füüsilist isikut (Art 3 (1)).

[18] X-tee on tehniline ja organisatsiooniline keskkond, mis võimaldab korraldada asutuste ja isikute vahelist turvalist ja tõestusväärsust tagavat internetipõhist andmevahetust ning turvalist juurdepääsu riigi infosüsteemile. (Vabariigi Valitsuse 24.04.2008 määrus nr 78 "Infosüsteemide andmevahetuskiht", § 2).

[19] Komisjon koostas pakkumiskutse ID-kaardi lähiuuringute teostamiseks ja otsustas laekunud vastuste põhjal, et lähiuuringu viib läbi AS Aprote ning ID-kaardi tehnoloogilise lähteuuringu Küberneetika AS.

15.02.1999. aastal võeti Eesti Vabariigis vastu isikut tõendavate dokumentide seadus ja märtsis 1999 moodustati Eesti Informaatikakeskuse käskkirjaga ID-kaardi töörühm standardite koostamiseks ja eksperthinnangute andmiseks ID-kaardi valdkonnas. Kodakondsus- ja Migratsiooniamet korraldas riigihanke konkurssi ID-kaardi pilootprojekti[20] tarbeks. Novembris 1999 teatati, et ID-kaardid tulevad kasutusele 2 aasta pärast ning siseminister andis välja käskkirja, millega moodustati isikutunnistuse kasutuselevõtmise kava väljatöötamise töörühm.[21]

Paralleelselt Eestis toimuvaga tegeldi digitaalallkirjade regulatsiooni loomisega ka Euroopa Liidu tasandil. **Digitaalallkirjade** regulatsioon tekkis Euroopa Liidu tasandil suuresti **direktiiviga 1999/93/EÜ**, mis realiseerus peale elektroonilisi allkirju käsitlevate õigusaktide vastuvõtmiseks ettepaneku[22] tegemist Euroopa Komisjoni teatises "Turvalisuse ja usalduse tagamine elektroonilises sides – digitaalallkirju ja krüpteerimist käsitleva Euroopa raamistiku poole“[23].

Mitmed liikmesriigid olid selleks ajaks juba vastu võtnud või alustanud ettevalmistavate tegevustega, et vastu võtta elektroonilisi allkirju käsitlevad riiklikud õigusaktid. Seda peeti elektroonilise kaubanduse kasvu üheks olulisemaks eelduseks ning tähtsaks poliitiliseks vajaduseks, et tagada elektrooniliste tehingute usaldusväärsus.[24]

Kuivõrd Euroopa Liidu vaatenurgast kujutasid riiklike õigusaktide erinevad nõuded endast ohtu siseturu tõhusale väljakujunemisele ja arengule – eriti elektrooniliste allkirjadega seotud toodetest ja teenustest sõltuvates valdkondades – nähti sealjuures ette ka ühtlustamismeetmed, mis pidid aitama ära hoida siseturu häireid valdkonnas, mida peeti Euroopa majanduses elektrooniliste tehingute tuleviku jaoks oluliseks. Üks keskne nõue selles raamistikus oli vajadus täpsustada elektrooniliste allkirjade õiguslikku seisundit, et tagada nimetatud allkirjade sageli küsitavaks peetud juriidiline staatus. Selliselt jõuti Euroopa Parlamendi ja

[20] Pilootprojekt kestvusega 6 kuud ja algusega 1. oktoobril 1999 anti teostamiseks Küberneetika AS-le.
[21] Arvutivõrgus: http://id.ee/?id=30651 (18.04.2015).
[22] Official Journal C 325 , 23/10/1998, lk 5-6.
[23] Opinion of the Economic and Social Committee on the "Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market". On 23 April 1999 the Council decided to consult the Economic and Social Committee, under Article 100a of the Treaty establishing the European Community, on the above-mentioned proposal. Official Journal C 169, 16/06/1999. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51999AC0457 (23.04.2015).
[24] Euroopa Parlamendi ja nõukogu 13. detsembri 1999. aasta direktiiv 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta, EÜT L 13, 19.1.2000, lk 12.

nõukogu poolt läbi vajaduse edendada digitaalallkirjade õiguslikku tunnustamist ning tagada digitaalallkirjaga toodete, seadmete ja teenuste vaba ringlus Euroopa Liidu ühtsel turul, 1999. aasta detsembris elektroonilisi allkirju käsitleva direktiivi vastuvõtmiseni.

Üldjuhul ei kehtestata õigusakte turunõudluse loomiseks ning seda ei tehtud ka kõnealuse direktiivi puhul, kuid direktiiviga pidi siiski kaasnema suurem õiguskindlus seoses elektrooniliste allkirjade ja seotud teenuste kasutamisega. Selles mõttes pani direktiiv aluse usaldusele, mis võimaldas turul areneda. Samas oli direktiivi digiallkirja definitsioon praktikas tõlgendatav ka selliselt, et digiallkiri loeti *de facto* identimisvahendiks[25], kuna seda kasutati elektroonsete andmete ehtsuse tõendamiseks, millest hilisema eIDAS määruse kontekstis on saanud osalt e-identimise komponent[26] – seega pandi direktiiv 1999/93/EÜ kohase digiallkirja regulatsiooniga teatud mõttes tahtmatult alus eID tekkele.

1.3.2. Arengu-aastad 2000-2009

8. märtsil 2000 võttis Eesti Vabariigi Riigikogu vastu digitaalallkirja seaduse[27] (edaspidi DAS), millega sätestati esmakordselt digitaalallkirja kasutamiseks vajalikud tingimused ning sertifitseerimisteenuse ja ajatempliteenuse osutamise üle järelevalve teostamise kord. Vastavalt seadusele defineeriti digitaalallkiri kui "tehniliste ja organisatsiooniliste vahendite süsteemi abil moodustatud andmete kogum, mida allkirja andja kasutab, märkimaks oma seost dokumendiga[28]" ja sätestati, et digitaalallkiri koos selle kasutamise süsteemiga peab võimaldama üheselt tuvastada isiku, kelle nimel allkiri on antud, kindlaks teha allkirja andmise aja ning siduma digitaalallkirja andmetega sellisel viisil, mis välistab võimaluse

[25] Direktiiv 1999/93/EÜ artikkel 2 p 1: *elektrooniline allkiri* – elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mida kasutatakse ehtsuse tõendamiseks.
Vs eIDAS määrus (EL) nr 910/2014 artikkel 3 p 10: *e-allkiri* – elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mida allkirja andja kasutab allkirja andmiseks.

[26] E-identimisel kasutatakse elektroonilisi isikutuvastusandmeid, mis tähistavad üheselt füüsilist või juriidilist isikut või juriidilist isikut esindavat füüsilist isikut ning seejuures autentimiseks loetakse elektroonilist protsessi, mis võimaldab füüsilise või juriidilise isiku e-identimist või elektrooniliste andmete päritolu ja tervikluse kinnitamist, mis on mõnevõrra sarnane direktiivis 1999/93/EÜ elektroonilsie allkirja toime määratlusega (andmete kasutamine ehtsuse tõendamiseks). Seetõttu on eIDAS määruses tehtud selgelt vahet e-identimisel ja e-allkirjal, kuivõrd praktikas tekkis ka eksperttasemel määruse eelnõu läbirääkimiste käigus mitmeid arusaamatusi e-identimise eristamisest varasemast (direktiivis 1999/93/EÜ reguleeritud) elektroonilisest allkirjastamisest.
Elektrooniliste allkirjade ja e-identiteedi selgele vahettegemisele viitab ka artikkel Gerhard Jakisch'i sulest „E-Signature versus E-Identity: the Creation of the Digital Citizen". Database and Expert Systems Applications. IEEE Xplore Digital Abstract, 2000, p. 312-316.

[27] Seadus jõustus 2000. aasta 15. detsembril.

[28] Digitaalallkirja seadus, § 2 lg 1. RT I 2000, 26, 150.

tuvastamatult muuta andmeid või nende tähendust pärast allkirja andmist[29]. Selles oli lähtutud juba e-allkirja direktiivi 1999/39/EÜ määratlustest, ehkki direktiiv kasutas mõistetena "elektroonilist allkirja"[30] ja "täiustatud elektroonilist allkirja"[31].

Võimaldamaks digitaalallkirja andmist, nähti meie digitaalallkirja seaduses ette sertifikaat kui dokument, mille avalik võti on seotud üheselt füüsilise isikuga. Isikliku ja avaliku võtme moodustajaks loeti sertifikaadi taotleja või vastavalt tema soovile ja pooltevahelisele kokkuleppele sertifitseerimisteenuse osutaja või muu isik või asutus[32]. Sama defineerib ka e-allkirja direktiiv, mille kohaselt on sertifikaat elektrooniline tõend, mis seob allkirja ehtsuse tõendamiseks vajalikud andmed isikuga ja kinnitab selle isiku samasust[33]. Samuti tegi DAS direktiivist juba sammukese edasi ning lõi aluse ka ajatemplile[34], mille üleeuroopaline regulatsioon tekib alles eIDAS määrusega. Sealjuures asutati Vabariigi Valitsuse poolt sertifitseerimise riiklik register[35], et pidada arvestust teenuste osutajate üle ning tagada ajatempliteenuse osutajate poolt väljaantavate ajatemplite ajalise järgnevuse võrreldavus registri vastutava töötleja kehtestatud täpsusega. Tegemist oli olulise sammuga edasi, kuna e-allkirja direktiiv ajatempli ega teiste usaldusteenuste reguleerimist ei käsitlenud.

12. juunil 2001 võeti vastu isikut tõendavate dokumentide seaduse ja digitaalallkirja seaduse muutmise seadus. Siseminister ja SA Vaata Maailma esindajad, EMT ning Hansapanga, Eesti Ühispanga ja Eesti Telefoni juhid kirjutasid 25. septembril 2001 alla koostöömemorandumile ID-kaardi laialdaseks rakendamiseks, millega tõmmati riikliku identiteedi kasutusvald-kondade arendamise meekonda tugevalt kaasa erasektor.

ID-kaardi ehk elektroonilise isikutunnistuse kohustuslikkuse üle peetud poliitiline diskussioon jõudis 2001.a lõpuks koalitsioonipartnerite vahelisele kokkuleppeni, mille tulemusena on ID-kaart käesoleva ajani EV residendile kohustuslik isikut tõendav dokument.

[29] Digitaalallkirja seadus, § 2 lg 3. RT I 2000, 26, 150.
[30] Euroopa Parlamendi ja nõukogu direktiiv 1999/93/EÜ art 2 p 1.
[31] *Ibid*., art 2 p 2.
[32] Digitaalallkirja seadus, § 7 lg 1. RT I 2000, 26, 150.
[33] Euroopa Parlamendi ja nõukogu direktiiv 1999/93/EÜ art 2 p 9.
[34] S.o tehniliste ja organisatsiooniliste vahendite süsteem, mille abil moodustub andmete kogum, mis tõendab dokumendi olemasolu kindlal ajahetkel.
[35] Registri vastutavaks töötlejaks määrati Teede- ja Sideministeerium.
Sertifitseerimise riikliku registri asutamine ja pidamise põhimäärus. Vastu võetud 12.12.2000 nr 416. Kehtetu – RT I 2009, 63, 413 – jõust. 26.12.2009.

28. jaanuaril 2002 anti kätte esimesed ID-kaardid[36] ning 07. oktoobril 2002 andsid Tartu ja Tallinna linnapead Andrus Ansip ja Edgar Savisaar esimesed digitaalallkirjad[37]. Sellega oli alguse saanud elektrooniline identifitseerimine ning kujunenud uus mõiste elektrooniline identiteet (eID).

Samal ajal arutleti Euroopa Liidus endiselt tihedalt liikmesriikide elektrooniliste identiteetide koostalitlusvõime puudumise üle. Oli liikmesriike, kes juba rakendasid elektroonilise identifitseerimise süsteeme juurdepääsuks liikmesriikide riigiasutuste elektroonilistele teenustele ja –menetlustele, tehnilised vahendid varieerusid aga suuresti, isegi kui üldiseks suundumuseks on kasutada elektroonilisi ID-kaarte. Liikmesriigid olid elektroonilise identifitseerimise vahendeid rakendanud seni omavahelise kooskõlastamiseta. Poliitilisel tasemel kutsuti 2005. ja 2007. aasta ministrite deklaratsioonidega[38] üles rakendama Euroopas koostalitlusvõimelist kasutaja tuvastamise süsteemi.

See oli oluline ühtse turu kasvava killustumise ärahoidmiseks. Euroopa Komisjon tegi 20. novembri 2007. aasta teatises[39] „21.sajandi Euroopa ühtne turg" ettepaneku võtta vastu **digitaalallkirju ja e-autentimist käsitlev tegevuskava**[40]. Tegevuskava eesmärk oli abistada liikmesriike vastastikku tunnustatud ja koostalitlusvõimeliste digitaalallkirjade ja elektroonilise identifitseerimise lahenduste rakendamisel, et seeläbi hõlbustada piiriüleste avalike teenuste osutamist elektroonilises keskkonnas. Otsustati, et ette tuleb näha konkreetsed meetmed digitaalallkirjade ja elektroonilise identifitseerimisega seoses. Tegevuskava oli suunatud peamiselt e-valitsuse rakendustele, kuid selles nähti potentsiaalset kasu ka ärirakendustele, niivõrd kuivõrd kasutusele võetavaid vahendeid saab kasutada ka ettevõtetevaheliste ning ettevõtja ja tarbija vaheliste tehingute puhul.

2008. aasta märtsi kevadisel Euroopa Ülemkogul teatasid riigipead ja valitsusjuhid, et digitaalallkirjade ja e-autentimise piiriüleste koostalitlusvõimeliste lahenduste kasutusele võtmine on ühtse e-turu toimivuse parandamiseks olulise tähtsusega.

---

[36] Neid väljastasid tol ajal ka Hansapanga ja Ühispanga kontorid.
[37] Arvutivõrgus: http://et.wikipedia.org/wiki/Eesti_ID-kaart (20.03.2015).
[38] Arvutivõrgus: http://www.umic.pt/images/stories/noticias/051124declaration.pdf (28.03.2015) ja http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=392 (28.03.2015).
[39] KOM(2007) 724 lõplik.
[40] 21.sajandi Euroopa ühtne turg. KOM(2007) 724 lõplik, lk 10.
E-autentimist mõistetakse siin *olemi* autentimisena, st elektroonilise identifitseerimisena. Dokumendis kasutatakse terminit „elektrooniline identifitseerimine", et selgemalt eristada olemi ja andmete autentimist.

1.3.3. Uus areng 2010-2014 – Euroopa digitaalne tegevuskava

Eesti oli esimene riik Euroopa Liidus, kus e-autentimise ja digiallkirjastamise raamistik ja tehnilised lahendused välja töötati ning kus neid kasutatakse ulatuslikult nii avalikus kui ka erasektoris.[41] Seetõttu on olnud ka Eesti riigi huvi, et meie lahendused oleksid koosvõimelised Euroopa tasandil kokkulepitud või kokkulepitavate lahendustega. Ühelt poolt on oluline, et üleeuroopalised kokkulepped tagaksid nii tehnilisel, protsesside kui ka õiguslikul tasandil kindluse, teiselt poolt, et me ei pea oma valitud lahendustes ja põhimõtetes tegema olulisi kannapöördeid. Eestil on tänu arvestatavale e-autentimise ja digitaalallkirjastamise kogemusele eduka e-riigi kuvand ja meie arvamust peetakse EL infoühiskonna küsimustes oluliseks. Oma Euroopa Liidu poliitika 2011–2015 tegevuskavas on Eesti otsustanud avaldada survet, et komisjon käivitaks e-allkirja direktiivi ülevaatuse[42]. 2011. a juunis toimunud Euroopa Liidu poliitika informatsiooni- ja kommunikatsiooni tehnoloogia (IKT) ja e-teenuste arutelurühm otsustas, et Eesti koostab Majandus- ja Kommunikatsiooniministeeriumi juhtimisel Euroopa Komisjonile esitamiseks ühtse kirjaliku sisendi/ettepaneku digiallkirja ja e-autentimise kohta[43]. Eesti ettepaneku koostamisel võeti aluseks Eesti käibelolev metoodika ning valmimisjärgus Eesti piiriülese autentimise tugi[44].

2010. aastal jõudis Euroopa Komisjon ühtse "Euroopa digitaalse tegevuskava"[45] väljatöötamiseni, mis on mh ka üks Euroopa 2020 strateegia seitsmest suurprojektist[46]. Euroopa digitaalse tegevuskava abil püütakse määrata kindlaks, kuidas kasutada maksimaalselt ära IKT sotsiaalset ja majanduslikku potentsiaali. Selles leitakse, et vaatamata ühtset turgu käsitlevate olulistele õigusaktidele, mis on seotud e-kaubanduse, e-arvete ja e-allkirjadega, on tehingud digitaalses keskkonnas endiselt liiga keerulised ning liikmesriikides ei rakendata eeskirju järjekindlalt. Isiku autentimise kõige üldisem vorm on endiselt salasõna kasutamine. Paljude rakenduste puhul sellest piisab, kuid üha enam on vaja turvalisemaid

[41] Eesti Euroopa Liidu poliitika 2011–2015.

[42] 2010. aastaks oli juba teada, et 2011. a direktiivi uut versiooni oodata ei ole ja et see võib jääda 2012 Taani eesistumisperioodi. Eesti saatis oma kirjaliku sisendi Euroopa Komisjonile avaliku konsultatsiooniprotsessi käigus 2011. a kevadel.

[43] See tähendas meile sobivate lahenduste väljapakkumist, mis direktiivis kajastust peaksid leidma. Põhieesmärk oli mõjutada e-allkirja direktiivi ja eriti selle e-autentimise osa sisu, mis eeldas ka riigisiseselt kokkuleppele jõudmist, millist isikutuvastuse turvataset ja milliseid autentimisvahendeid on Eesti valmis aktsepteerima, teades, et oleme Eestis harjunud tugeva, riikliku isikutuvastusega ning raske on samastuda liikmesriikidega, kes aktsepteerivad ka madalama turvatasemega isikutuvastust.

[44] Arvutivõrgus: https://www.eid-stork.eu/pilots/pilot4_EE.htm (28.02.2015)

[45] Arvutivõrgus: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245 (28.032015)

[46] EUROPE 2020. A strategy for smart, sustainable and inclusive growth. COM(2010) 2020 final, lk 5-6. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

lahendusi[47]. Kuna subsidiaarsuse printsiibist lähtuvalt ei saa Euroopa Liit liikmesriikidele ette kirjutada, milliseid elektroonilisi identiteedivorme on neis lubatud kasutada ning juba kasutusel olevaid lahendusi on palju, vajab Euroopa standarditel põhinevat koostalitlusvõime raamistikku. Sobiva meetmena nähakse selleks **e-allkirja käsitleva direktiivi läbivaatamist**[48], et tagada õiguslik raamistik **turvalise e-autentimise** süsteemide piiriüleseks tunnustamiseks ja koostalitluseks.

Samas vajavad ületamist veel piirangud, mis takistavad ettevõtjate ja kodanike liikuvust, kuivõrd enamik **avalikke võrguteenuseid ei toimi piiriüleselt**. Mitmed ühtse turu algatused ja õigusaktid, nagu näiteks teenuste direktiiv[49] või e-hangete tegevuskava[50], eeldavad ettevõtjate võimalust ametiasutustega suhelda ja äriasju ajada just elektrooniliste vahendite abil ning piiriüleselt[51]. Seetõttu sõnastab Euroopa digitaalne tegevuskava juba meetme täpsusega praktiliste piiriüleste e-identimise ja e-autentimise teenuste rakendamise vajaduse koos autentimiseks vajalike turvatasemete vastastikuse tunnustamisega. Komisjon lubab esitada 2012. aastaks ettepaneku Euroopa Parlamendi ja nõukogu otsuse kohta, et tagada e-identimise ja e-autentimise vastastikune tunnustamine kogu Euroopa Liidus[52]. Aluseks võetakse kõikides liikmesriikides pakutavad veebipõhised autentimisteenused, mis võivad kasutada kõige ajakohasemaid avaliku või erasektori väljastatud ametlikke dokumente. See oli täpselt eesmärk, mida Eesti eelneva tegevuse ja oma 2011-2015 Euroopa Liidu tegevuskava-põhiste sammudega taotlenud oli. 2011. aasta septembris saatis Eesti Vabariik Euroopa Komisjoni juurde riikliku eksperdi e-identimise ja e-autentimise vastastikuse tunnustamise meeskonda uut regulatsiooni välja töötama[53].

Seega võib öelda, et Eesti on reaalselt mõjutanud läbi oma tegevuse Euroopa Liidus Euroopa digitaalse arengukava kujundamist ning Eestil on olnud oluline roll Euroopa digitaalse turu parendamises.

---

[47] Komisjon on seepärast esitanud ettepaneku, mis käsitleb Euroopa strateegiat identiteedi haldamise kohta Stockholmi programmi alusel, KOM(2010) 171.
[48] Euroopa digitaalne tegevuskava. KOM(2010)245 lõplik. Meede nr 3, lk 11.
[49] Euroopa Parlamendi ja nõukogu direktiiv 2006/123/EÜ teenuste kohta siseturul. ELT L 376, 27.12.2006, lk 36–68. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32006L0123&rid=1 (28.03.2015).
[50] Arvutivõrgus: http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/actionplan/actionplan_en.pdf (28.03.2015).
[51] Tulevaste avalike võrguteenuste eelduseks on eespool kirjeldatud tõhusad ja koostalitlusvõimelised identiteedi haldamise ja autentimise raamistikud ja vahendid.
[52] Euroopa digitaalne tegevuskava. KOM(2010)245 lõplik, meede 16, lk 33.
[53] Eesti Euroopa Liidu poliitika 2011–2015 tegevuseesmärgid. Lisa 1, lk 3.

1.3.3.1. eID paralleelne areng Eestis

Eestis oli selleks ajaks toimunud 2000-ndate algusega võrreldes juba oluline edasiminek – digitaalse isiku tõendamise vormid olid vahepeal oluliselt täienenud. Digitaalseteks isikut tõendavateks dokumentideks olid lisaks isikutunnistusele saanud tänapäevased elamisloa-kaart, digitaalne isikutunnistus ja e-residendi digitaalne isikutunnistus, millele kõigile on kantud digitaalset tuvastamist ning digitaalset allkirjastamist võimaldavad sertifikaadid.

Digitaalne isikutunnistus on Eesti Vabariigis kasutusel aastast 2009. See on defineeritud isikut tõendavate dokumentide seaduse (ITDS) § 19^1 kohaselt kui digitaalsete andmetega isikutunnistus. Digitaalse isikutunnistuse väljaandmises nähti võimalust elektroonilises keskkonnas kasutatavate dokumentide paljususe tekkimiseks, mis tagaks senisest kindlama ligipääsu elektroonilistele teenustele.[54]

Digitaalne isikutunnistus on seega alates 2009. aasta 30. juulist paralleelselt isikutunnistusega elektrooniliselt kasutatav kiipkaart, millega saab elektroonilises keskkonnas oma isikut tuvastada ja digitaalallkirja anda. Digitaalsel isikutunnistusel ei ole isiku fotot ning seetõttu ei saa teda kasutada isikut tõendava dokumendina väljaspool elektroonset keskkonda.

Erasektori algatusena oli **mobiil-ID** kasutusel juba 2007. aastast. Pideva elektroonilise asjaajamise arengu ja selle kasutamisvõimaluste laienemisega oli mobiil-ID lahendusele kindlustatud juba piisavalt lai kasutajaskond, kelle abil nähti perspektiivi ja vajadust luua täiendav alus isiku elektrooniliseks tuvastamiseks ning toetada uudset lahendust, mis aitaks kaasa Eesti infoühiskonna kui terviku arengule ka kaugemas perspektiivis.[55] Näiteks olid juba laialt levinud mobiilsed seadmed (nutitelefonid ja tahvelarvutid), kus seni ID-kaardi lugeja puudumise tõttu ei olnud elektroonset isikutuvastamist nõudev asjaajamine võimalik. Mobiil-IDst sai täiendus riigi poolt kiipkaardi vormis väljastatavale digitaalsele isikutunnistusele, võimaldades edaspidi ka mobiiltelefoni abil isiku digitaalset tuvastamist ja digitaalset

[54] Isikut tõendavate dokumentide seaduse, konsulaarseaduse, karistusseadustiku, riigilõivuseaduse, välismaalaste seaduse ja kodakondsuse seaduse muutmise seadus 395 SE seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/df3dd438-72e6-bdd9-acb3-f3aac7d2f025/Isikut-t%C3%B5endavate-dokumentide-seaduse,-konsulaarseaduse,-karistusseadustiku,-riigil%C3%B5ivuseaduse,-v%C3%A4lismaalaste-seaduse-ja-kodakondsuse-seaduse-muutmise-seadus/ (30.04.2015)

[55] Isikut tõendavate dokumentide seaduse ja teiste seaduste muutmise seaduse eelnõu seletuskiri, 844 SE II. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/5422b8d0-33ed-7890-b56a-7452b83d8b56/Isikut-t%C3%B5endavate-dokumentide-seaduse-ja-teiste-seaduste-muutmise-seadus/ (30.04.2015).

allkirjastamist. Mobiil-ID hakkas välja andma ja haldama PPA.

Samal ajal loodi alus ka kolmanda elektroonilisi isikuandmeid kandva isikutunnistuse vahendi kasutuselevõtuks – selleks sai välismaalase **elamisloakaart**. Selle vajadus oli spetsiifilisemalt seotud rahvusvahelise sõjalise koostöö seaduse alusel Eestis viibivate välisriigi relvajõudude liikmete või relvajõude saatvate tsiviilisikute ja nende isikute ülalpeetavate igapäevaeluliste probleemidega, nagu võimaluse puudumine teha soovitud ulatuses pangatehinguid[56], esinesid probleemid mobiilioperaatoriga lepingute sõlmimisel[57], puudus võimalus kasutada ühistransporti samadel tingimustel ning paindlikkusega nagu isikutunnistust omavatel isikud või kasutada muid isikutunnistuse olemasolu eeldavaid ettevõtjate või riigi elektroonilisi teenuseid.[58] Leiti, et ka nemad vajavad igapäevaseks tõrgeteta asjaajamiseks Eestis üldlevinud füüsilist ja digitaalset isikut tõendavat dokumenti, mis võimaldaks neil oma isikut tõendada nii füüsiliselt kui elektroonilises keskkonnas ning millelt nähtuks nende Eestis viibimise seaduslik alus. Selleks võeti 25.11.2010 vastu ITDS muudatused, mis lõid aluse Eesti siseriikliku isikut tõendava dokumendi ja digitaalse isikut tõendava dokumendi väljaandmiseks ka neile Euroopa Liidu kodanikele ja kolmandate riikide kodanikele, kes viibivad Eestis rahvusvahelise sõjalise koostöö raames, ning nende isikute poolt ülalpeetavatele isikutele.

24. aprillil 2014 lisandus eelnevale juba neljas, kuid kontseptuaalselt täiesti unikaalne elektroonilist identiteeti kandev isikutunnistuse vahend – Vabariigi Valitsuse kabineti istungil kiideti just siis heaks uus kontseptsioon[59] mitte residentsetele digitaalse isikutunnistuse väljaandmiseks ehk e-residentsuse loomine. Arvestades Eesti rahvastiku vananemist ja Eesti vähest võimekust konkureerida kõrgelt kvalifitseeritud oskustööjõu pärast atraktiivsemate

[56] Pangad ei võimalda paroolikaardiga teha enam muid kui väikese summaga tehinguid, ning paroolikaardi ja PIN-kalkulaatori kasutamisest võidakse üldse loobuda.

[57] Eraettevõtjatel on olemuslikult õigus valida kliente ja keelduda nende isikute oma kliendiks võtmisest, kelle suhtes nad ei tunne piisavalt usaldust (v.a konkurentsiseaduses sätestatud juhul, kui nad on turgu valitsevas seisundis). Kui kliendiks soovib saada isik, kelle isikut ja riigis viibimise seaduslikkust tõendavaks dokumendiks on üksnes välisriigi reisidokument, nagu see oli enne 2011. aastat rahvusvahelise sõjalise koostöö raames Eestis viibivate isikute puhul, oli ettevõtja jaoks arvestatav risk, et võlgu jäämise korral võib selline isik lahkuda ootamatult püsivalt välisriiki, kust võla kättesaamine võib kujuneda ebamõistlikult raskeks või võimatuks.

[58] Isikut tõendavate dokumentide seaduse ja teiste seaduste muutmise seaduse eelnõu seletuskiri, 844 SE II. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/5422b8d0-33ed-7890-b56a-7452b83d8b56/Isikut-t%C3%B5endavate-dokumentide-seaduse-ja-teiste-seaduste-muutmise-seadus/ (30.04.2015).

[59] Mitteresidentidele digitaalse isikutunnistuse väljaandmine: e-residentsuse loomine. Kontseptsioon. Arvutivõrgus: https://www.siseministeerium.ee/public/e-residendi_digi_id_Lisa_1_kontseptsioon.pdf (28.03.2015).

riikidega, otsiti lahendusi isikute kaasamiseks Eesti majanduse ja ühiskonna arengusse valdkondades, kus see on olemuslikult võimalik, ilma et eeldaks nende isikute Eestisse elama asumist[60], mida e-residentsuse kontseptsioon pakkus. Kontseptsiooni kohaselt on Eesti e-resident välismaalane, kellele Eesti on loonud digitaalse identiteedi tema kodakondsusjärgse riigi poolt väljaantud ja Eesti poolt tunnustatud isikut tõendavasse dokumenti kantud identiteediandmete alusel ning andnud digitaalse isikut tõendava dokumendi – **e-residendi digitaalse isikutunnistuse**. E-residentsus loob võimaluse kasutada e-teenuseid Eesti digitaalse dokumendiga. See võimaldab Eestis tegutsevale välismaalasele ja väikeettevõtjale tuvastada enda isikut ja anda allkirja ilma selleks füüsiliselt kohale tulemata ja paberdokumente vormistamata. Näiteks saab e-resident oma elektroonilist identiteeti kasutades asutada äriühingut, teha maksu- ja tollialaseid elektroonilisi toiminguid ning kasutada oma eID-d riigiga suhtlemisel.

Seoses e-residentsuse loomisega tuli õigusselguse huvides ja väärkasutuse vältimiseks täiendada isikut tõendavate dokumentide seadust[61]. Lisandus regulatsioon e-residendile digi-ID väljastamiseks, selle kasutuse õiguspärasuse üle järelevalve teostamiseks, kehtivuse peatamiseks ja kehtetuks tunnistamiseks. „Eesti infoühiskonna arengukava 2020“[62] üks tegevussuund näeb ette pakkuda teenuste baastaristu arendamisel välisriikide kodanikele n.ö virtuaalset residentsust – ehk võimaldada neil elektroonilise ID väljastamisega kasutada Eesti e-teenuseid ja turvalist andmevahetust. Aastaks 2020 peaks Eestil olema vähemalt 5000[63] e-residenti.

Seega võib öelda, et Eestis on kasutuses praktiliselt kõik olemasolevad elektroonilise isikutuvastuse võimalused nii oma kodanikele kui välismaalastele.

[60] Ruth Annus. E-residentsus. Juridica, 2014, nr 10, lk 741.
[61] Kuritegevus digitaalses ruumis ei mõjuta mitte üksnes otseseid kannatanuid, vaid võib ohustada ka kodanike ja ettevõtete usaldust digitaalsete süsteemide vastu, mis on ühiskonna ja majanduse jaoks kriitilise tähtsusega. Vt Strategy to Combat Transnational Organized Crime. US 2011, p. 8. Arvutivõrgus: https://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf (01.05.2015).
[62] Vabariigi Valitsuse 18. novembri 2013. a korraldus nr 509. RT III, 19.11.2013, 14.
[63] Eesti infoühiskonna arengukava 2020, lk 21.

1.3.4. EIDAS määruse loodav muutus

Euroopa Komisjon viis 2012. aastal läbi e-valitsuste võrdlusuuringu[64], millest selgus, et Eestis on ligipääs riigi pakutavatele e-teenustele ja infole Euroopa Liidu parimate seas. Olulisimad üleeuroopalised probleemid on piiriülesel e-teenuste osutamisel valdavas osas seotud elektroonse identiteediga. Seda kinnitavad mitmed uuringud[65]. Riigisiseselt on enamikus liikmesriikides autentimise ja digiallkirjastamise küsimused lahendatud, kuid selleks, et erinevad tehnilised ja protseduurilised lahendused toimiks ka üle riigipiiride, on vaja luua süsteem nende üleeuroopaliseks koosvõimeks. Selleks juhtis komisjon juba paralleelselt eIDAS määruse koostamisprotsessi, et tagada nii füüsilistele isikutele kui ettevõtetele võimalus kasutada riiklike elektrooniliste IDde pakutavat juurdepääsu avalikele teenustele piiriüleselt.

Digiallkirjade puhul on üleeuroopaline õiguslik raamistik loodud 1999. aastal vastu võetud elektroonilise allkirja direktiiviga 1999/93/EÜ, kuid põhilised probleemid seisnevad siiski digitalallkirjade vastastikuse tunnustamise ja piiriülese koostoime puudustega – standardimisdokumente oli liialt palju ja neil puudus äritegevust ergutav toime[66]. Teadaolevalt esimene digitaalallkirjastatud rahvusvaheline kokkulepe maailmas sõlmiti 2013. aasta 10. detsembril[67] Eesti ja Soome peaministrite vahel, mil Andrus Ansip ja Jyrki Katainen allkirjastasid vastavalt Eesti Vabariigi ja Soome Vabariigi nimel enda ID-kaarte kasutades digitaalselt koostöömemorandumi kahe riigi info- ja kommunikatsioonitehnoloogia valdkonna koostöö edendamiseks.

Autentimist käsitlev EL regulatsioon puudus täielikult. Eesti sõnastas oma Euroopa Liidu poliitika 2011-2015 raamdokumendis eesmärgi EL-i regulatsiooni loomiseks e-autentimise

---

[64] Public Services Online "Digital by Default or by Detour?". Assessing User Centric eGovernment performance in Europe – eGovernment Benchmark 2012. Arvutivõrgus: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/eGov%20Benchmark%202012%20insight%20report%20published%20version%200.1%20_0.pdf (03.04.2015).
Uuringu käigus analüüsiti infot 28´000 internetikasutajalt 32 riigis.

[65] Thomas Myhr. Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution or I am 621216-1318, but I am also 161262-43774. Do you know who I am?. Information Security Technical Report. May 2008. Volume 13, Issue 2. Pp 76-82; Siddharta Arora. National e-ID card schemes: A European overview. Information Security Technical Report. May 2008. Volume 13, Issue 2. Pp 46-53; Tobias Mahler. Governance Models for Interoperable Electronic Identities. Journal of International Commercial Law and Technology, 2013. Vol. 8, No. 2, p. 148-159.

[66] Feasibility Study on an Electronic Identification, Authentication and Signature Policy (IAS). European Union 2013, p 66.

[67] Arvutivõrgus: http://www.id.ee/?id=36540 (13.03.2015).

vallas ning digiallkirjade piiriülese toimimise tagamise praktikas[68]. Eesti deklareeris samuti vajadust siseturu üldise raamistiku uuendamiseks, mis muu hulgas hõlmaks siseturu reguleerimiseks senisest enam otsekohaldatavate õigusaktide kasutamist, Euroopa Komisjoni suuremat rolli nelja vabaduse[69] toimimise järelevalvel ja rakendamisel, ning mehhanismide loomist, mis tagaksid, et nende nelja vabaduse järgimine ja rakendamine riiklikul ja regionaalsel tasandil oleks tõhusalt tagatud.[70]

23. juuli 2014. a võeti vastu Euroopa Parlamendi ja Euroopa Nõukogu **määrus nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul** (edaspidi viidatud kui *eIDAS määrus* või *määrus*), millega tunnistati direktiiv 1999/93/EÜ kehtetuks. EIDAS määrus (*electronic IDentification and Authentication Services regulation*) avaldati Euroopa Liidu Teatajas 28. augustil 2014.a. Ees seisab veel avaldamisjärgne, nö alustatu lõpuleviimise protsess mitmete rakendusaktide väljatöötamise näol[71].

Määruse valdav osa sätteid jõustub 1. juulist 2016. Sellest alates peaksid kõigi ELi maade riigiasutused vastastikku tunnistama üksteise digiallkirju ning 2018. aastast ka e-identiteete. Sealjuures eksisteerib võimalus, kui komisjoni rakendusaktid valmivad ja saavad vastuvõetud tähtaegselt, osade liikmesriikide poolt eIDde vabatahtlikuks rakendamiseks juba 2015. a sügisest[72].

Antud määrus asendab kõiki Euroopa Liidu liikmesriikides kehtivaid ja mitte kooskõlas olevaid siseriiklikke seaduseid. EIDAS määrus toob mitmeid olulisi muutusi tulevikuks, mida käsitletakse käesolevas töös, tutvustades uusi reegleid elektroonilise identifitseerimise vahendite koostalitlusvõimeks ja vastastikuseks tunnustamiseks.

Esimene olulisem ja peamine muudatus eIDASe näol seisneb õigusliku raamistiku loomises, mis toetab liikmesriikide elektrooniliste isikutuvastusvahendite kasutust üleeuroopaliselt, olgu

[68] Vt Eesti Euroopa Liidu poliitika 2011–2015 tegevuseesmärki I-a lisas.
[69] Kaupade vaba liikumine, teenuste vaba liikumine, tööjõu vaba liikumine ja kapitali vaba liikumine.
[70] Eesti Euroopa Liidu poliitika 2011–2015, lk 9 p 1.
[71] Nt artikkel 8 lõike 3 kohaselt e-identimise süsteemide usaldusväärsuse tasemete määramiseks minimaalsed tehnilised kirjeldused, standardid ja menetluskord, artikkel 12 lõike 8 kohane koosvõimeraamistik. Määruse üldises kontekstis lisanduvad nimetatutele veel artiklite 22 lg 5, 23 lg 3, 27 lg 5 ja 37 lg 5 kohased rakendusaktid.
[72] EIDAS määruse artikkel 52 lõige 4 näeb ette, et ilma et see piiraks artikli 52 lõike 2 punkti c kohaldamist, võib liikmesriik otsustada, et muu liikmesriigi poolt artikli 9 lõike 1 kohaselt teada antud e-identimise süsteemi kohaseid e-identimise vahendeid tunnustatakse esimesena nimetatud liikmesriigis alates artikli 8 lõikes 3 ja artikli 12 lõikes 8 osutatud rakendusaktide kohaldamise kuupäevast. Asjaomased liikmesriigid teavitavad sellest komisjoni ja komisjon avalikustab nimetatud teabe.

see kas Eesti, Soome, Austria või Hispaania ID-kaardi lahendus. Ennekõike on määruse regulatsioon suunatud liikmesriikide avalikule sektorile, kohustades liikmesriike tunnustama teiste liikmesriikide elektroonilisi isikutuvastusvahendeid (eID-sid) ja võimaldama nende ligipääsu olemasolevatele elektroonilistele teenustele. Seeläbi aidatakse mh kaasa liikmesriikide elektrooniliste ID-de kasutusalade laienemisele, näiteks juba väljaantud Läti elektroonilise ID-kaardiga võib pääseda ligi Eesti e-riigiteenustele. Erasektor ei ole käesolevast määrusest küll otseselt puudutatud, kuid võimalus nendele, kes selles kasu näevad oma teenuste üleeuroopaliseks laiendamiseks, on olemas. Nagu ka varem viidatud komisjoni tellitud 2013. aasta uuringus "*Feasibility Study on an Electronic Identification, Authentication and Signature Policy (IAS)*[73]" märgiti, et varasemad ühenduse tasandi standardimisdokumentidel puudus äritegevust ergutav toime[74], näeb ka eIDAS määruse põhjenduspunkt 17 ette erasektori ergutamise määravuse arvestatava kasutusmahu saavutamiseks[75].

Teine olulisem muutus puudutab reegleid uutele teenustele – kui digitaalallkirja direktiiv lõi ennekõike õigusliku raamistiku elektrooniliste allkirjade kasutamiseks, siis eIDAS määrus toob välja ja reguleerib eraldi uut tüüpi usaldusteenused nagu e-tempel, e-ajatempel, registreeritud e-andmevahetusteenused ja veebisaitide autentimise sertifitseerimisteenused. EIDAS näeb varasemaga võrreldes selgesõnaliselt ette põhimõtte tehnoloogia neutraalsusest[76]. Määrus pakub ka stiimuleid, andes näiteks suurema õiguskindluse usaldada neid teenuseid, mis järgivad konkreetseid reegleid – mille eesmärk on parandada teenuste usaldusväärsust. Sel viisil on püütud tasakaalustada huvisid õigusliku prognoositavuse ja innovatiivsuse vahel. Samas ei ole õigusloomeline protsess veel lõpule jõudnud. Rakendusaktidega pannakse paika olulised tehnilised detailid. Küll aga on vastu võetud esimene komisjoni rakendusotsus (EL) 2015/296[77], millega kehtestatakse menetluskord liikmesriikidevaheliseks koostööks e-identimise valdkonnas vastavalt eIDAS määruse artikli 12 lõikele 7 ning tööversioonis on arutelu all artiklite 8 ja 9 lõike 1 otsuse eelnõu. Nende mõlema mõju Eesti e-identimissüsteemile käesolev töö 2. peatükis lähemalt analüüsib.

[73] Arvutivõrgus: http://ec.europa.eu/digital-agenda/en/news/feasibility-study-electronic-identification-authentication-and-signature-policy-ias-0 (21.04.2015).
[74] Vt käesoleva töö lk 22.
[75] Komisjon on näidanud eeskuju ja korraldanud selleks ise 2 eIDd puudutavat erasektorile suunatud teavitusüritust: 1) 19. novembril 2014 eIDAS Private Sector Engagement High Level Event "eID: a key to business growth and innovation" ja 2) 31. märtsil 2015 eIDAS Private Sector Engagement High Level Event "eID: emerging business cases".
[76] EIDAS määruse põhjenduspunktid 16 ja 27 ning artikkel 12 lõige 3(a).
[77] ELT L 53, 25.2.2015, lk 14-20.

2. EIDAS MÄÄRUSE KOHALDAMINE EESTIS

2.1. Määruse kohaldamine: EL lepingu art 5 ning määruse kohaldamisala

EV põhiseaduse täiendamise seadus (PSTS)[78] § 2 kohaselt kohaldatakse Eesti kuulumisel Euroopa Liitu Eesti Vabariigi põhiseadust, arvestades liitumislepingust tulenevaid õigusi ja kohustusi. EL-ga ühinemisel muutusid Eesti seaduste kõrval **otsekohaldatavaks** ka EL määrused, mida kohaldatakse üldiselt ning need on tervikuna siduvad ja vahetult kohaldatavad kõikides liikmesriikides. Määruse reguleerimisala ei saa Eesti seadustega reguleerida. Küll aga on võimalik, et EL määrus näeb ette siseriiklike rakendusaktide vastuvõtmise, millisel juhul tuleb EL määruse alusel vastu võtta vajalikud seadusemuudatused või Vabariigi Valitsuse määrused.[79]

Euroopa Liidu õiguse vahetu kohaldatavuse põhimõtet on käsitlenud Euroopa Liidu Kohtu 05.02.1963. a kohtuasjas 26/62 Van Gend en Loos[80]: "Vahetult liikmesriikide üksikisikutele võivad õigusmõju omada EL aluslepingute (Euroopa Liidu leping, Euroopa Liidu toimimise leping) sätted, kindlasti on vahetult kohaldatavad EL määrused ja teatud juhtudel EL direktiivid ja otsused." Eesti Vabariigi põhiseaduse täiendamise seaduse (PSTS) eelnõu seletuskiri peab PSTS § 2 puhul oluliseks EL määruste ja direktiividega arvestamist.[81]

Seega eIDAS määruse reguleerimisala ei saa Eesti oma seadustega (ümber)reguleerida, kuid antud määrusest tulenevatest kohustustest liikmesriikidele tuleb analüüsida vajadust käesoleva EL määruse alusel vastu võtta vajalikud seadusemuudatused või Vabariigi Valitsuse määrused.

Samuti on oluline märkida Euroopa Liidu lepingu[82] artikkel 5 kohase pädevuse kasutamise kohast **subsidiaarsuse ja proportsionaalsuse põhimõtte** silmaspidamist, mida on rakendatud ka eIDAS määruse puhul. Komisjon on analüüsinud ning leidnud, et eIDAS määruse eesmärke ei suuda liikmesriigid eraldiseisvalt piisavalt saavutada, küll aga saab neid meetme ulatuse tõttu paremini saavutada liidu tasandil. Sellest johtuvalt võib liit võtta meetmeid

[78] Eesti Vabariigi põhiseaduse täiendamise seadus. RT I 2003, 64, 429.
[79] EVPS kommenteeritud väljaanne. PSTS § 2 kommentaar p 8.1.
[80] Arvutivõrgus: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=87120&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2399729 (03.04.2015).
[81] EVPS kommenteeritud väljaanne. PSTS § 2 kommentaar p 15.
[82] Euroopa Liidu leping (konsolideeritud versioon). ELT C 326, 26.10.2012. Lk 13-46.

kooskõlas EL lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega – ning määruse põhjenduspunkt 76 sätestab, et eIDAS määrus ei lähe nimetatud eesmärkide saavutamiseks EL lepingu art 5 sätestatud proportsionaalsuse põhimõtte kohaselt vajalikust kaugemale. EIDAS määruse kohaldamisalana on määrus määratud **kohalduma liikmesriikide poolt teavitatud e-identimise süsteemide ja liidus asuvate usaldusteenuste osutajate suhtes**, kelleks käesoleva töö kirjutamise hetkel on Eesti Vabariigis sertifitseerimise registri andmetel[83] AS Sertifitseerimiskeskus ja GuardTime AS.

2.2. Määruse aluspõhimõtted

2.2.1. Kaupade ja teenuste vaba liikumine

EIDAS määruse peamiseid tugitalasid on Euroopa Liidu toimimise lepingu artiklist 114 tulenev eesmärk tagada Euroopa Liidus toimiv siseturg[84]. Nimelt sätestab EL toimimise lepingu art 114 lõikes 1, et seadusandliku tavamenetluse kohaselt ning pärast konsulteerimist majandus- ja sotsiaalkomiteega võtavad Euroopa Parlament ja nõukogu liikmesriikides nii õigus- kui ka haldusnormide ühtlustamiseks meetmed, mille eesmärk on siseturu rajamine ja selle toimimine. EIDAS regulatsiooni sügavam sisu seisneb, mitte e-ID-de ja usaldusteenuste turu ühtlustamises *per se*, vaid üldisemalt meetmete kehtestamises, mis toetavad EL siseturu ettevõtlust ja ergutavad piiriülest kaubandust – antud juhul läbi e-identimise ja usaldusteenuste regulatsiooni ühtlustamise. Nii viitavad eIDAS määruse mitmed põhjenduspunktidki selgelt majanduslikele eesmärkidele: läbi ühise aluse loomise turvalisele elektroonilisele suhtlusele kodanike, ettevõtjate ja ametiasutuste vahel suurendatakse avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse tõhusust liidus[85], tõstetakse esile internetipõhiste teenuste piiriülese kasutamise lihtsustamisega täielikult integreeritud digitaalse ühtse turu edendamist[86], märgitakse, et nõukogu on palunud komisjonil edendada digitaalset ühtset turgu sobivate tingimuste loomisega piiriüleste põhieelduste (näiteks e-identimise) vastastikuseks tunnustamiseks ning koosvõimelisteks e-valitsuse teenusteks kogu Euroopa Liidus[87], lisatakse, et elektrooniline takistus, mille tõttu kodanikud ei saa e-identimist enamasti kasutada enda autentimiseks teises liikmesriigis, sest nende koduriigi riiklikke e-

[83] Arvutivõrgus: http://sr.riik.ee/et/sp.html (22.03.2015).
[84] Euroopa Liidu toimimise lepingu konsolideeritud versioon. ELT C 326, 26.10.2012.
[85] eIDAS määruse põhjenduspunkt 2.
[86] *Ibid*., põhjenduspunkt 5.
[87] *Ibid*., põhjenduspunkt 6.

identimise süsteeme teistes liikmesriikides ei tunnustata, ei lase teenuseosutajatel siseturust täit kasu saada – vastastikku tunnustatavad e-identimise vahendid seevastu lihtsustavad paljude teenuste piiriülest osutamist siseturul ja võimaldavad ettevõtjatel piiriüleselt tegutseda, ilma et neil oleks palju takistusi avaliku sektori asutustega suhtlemisel[88] ning annavad suunise ergutada ka erasektorit vabatahtlikult kasutama teavitatud süsteemi kuuluvaid e-identimise vahendeid identimiseks, et muuta piiriülese juurdepääsu erasektori internetipõhistele teenustele ettevõtjate ja kodanike jaoks lihtsamaks[89]. Nendes väljendatud soov ja tahe viitab üheselt määruse eesmärgile anda tõuge Euroopa Liidu majaduse arengule ning muuta läbi e-identimise regulatsiooni ühtlustamise[90] kaupade ja teenuste tarbimine piiriüleselt hõlpsamini kättesaadavaks ja turvalisemaks, mis elavdaks tervikuna Euroopa Liidu majandust.

2.2.2. Tehnoloogia neutraalsus

EIDAS määruse kontekstis ei ole mõiste *tehnoloogia neutraalsus* iseseisvat defineerimist leidnud, kuid sellele viidatakse eID baaspõhimõtete raames läbivalt[91]. Teaduskirjanduses on Chris Reed[92] tehnoloogia neutraalsust käsitlenud kui potentsiaali neutraalsust[93], kus regulatsioon ei tohi olla diskrimineeriv konkreetse tehnoloogia suhtes, kuid samas ei või see ka pidurdada ühegi konkreetse tehnoloogia arengut[94]. Tehnoloogia neutraalsuse printsiipi on Euroopa Liidu regulatsioonide kontektsis kirjeldatud ka kui normi, et regulatsioonid ja EL poliitika peab olema ennekõike piisavalt üldine ja kaasteksti väline, kui et konkreetse tehnoloogia kirjeldus[95].

EIDAS määruses on põhjenduspunktis 27 deklareeritud, et antud määrus peaks olema tehnoloogiaküsimustes neutraalne ja tema õiguslik mõju saavutatav mis tahes tehniliste vahenditega eeldusel, et täidetakse käesoleva määruse tingimusi. Samas Euroopa Parlamendi

[88] eIDAS määruse põhjenduspunkt 9.
[89] *Ibid*., põhjenduspunkt 17.
[90] Sama määrus hõlmab paralleelselt ka usaldusteenuste regulatsiooni ühtlustamist liidu tasandil, mille raames tunnistatakse kehtetuks varasem e-allkirja direktiiv 1999/93/EÜ. Selle väärtus on laiemalt ühtsete ja otsekohalduvate reeglite kehtestamises kõigile 28-le liikmesriigile.
[91] Vt eIDAS määruse põhjenduspunkte 16 ja 27 ning artikkel 12 lg 3 punkti 1.
[92] Professor of Electronic Commerce Law, Centre for Commercial Law Studies, Queen Mary University of London.
[93] I.k. *potential neutrality*.
[94] Chris Reed. Taking sides on technology neutrality. *SCRIPTed* - A Journal of Law, Technology & Society, Vol. 4, Issue 3, p. 273.
[95] Edgar A. Whitley. On technology neutral policies for e-identity: A critical reflection based on UK identity policy. Journal of International Commercial Law and Technology, 2013. Vol. 8, No. 2, p. 134.

ja nõukogu direktiivi 2002/21/EÜ[96], elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta, põhjenduspunkti 18 kohaselt viidatakse tehnoloogia neutraalsusele kui põhimõttele, mille kohaselt ei soosita ega halvustata konkreetset liiki tehnoloogia kasutamist ega välistata proportsionaalsete meetmete võtmist teatavate konkreetsete teenuste edendamiseks, kui see on põhjendatud. Täiendavalt on Euroopa Komisjoni 14. oktoobri 2014 memo[97] järgi tehnoloogia neutraalsust käsitletud kui vajadust vältida nõudeid, mis võiksid järgida ainult ühe konkreetse tehnoloogia lahendusi.

Eelnevaid tõlgendusi ja näiteid kokku võttes võiks tehnoloogia neutraalsust mõista kui võimaldavat tegurit uute lahenduste väljatöötamiseks, millega ei pidurdata ühegi konkreetse tehnoloogia arengut, ent võimaldatakse vajadusel siiski teatavaid kitsendusi ja arengule mõju omavat reguleerimist, kedagi sihilikult sealjuures diskrimineerimata.

EIDAS määruse eesmärk üldise majanduse elavdamise juures on tõmmata e-identimise ja usaldusteenuste vahelisele koostööle maksimaalne hulk liikmesriike ning muuta juba liikmesriikides kasutatavad internetipõhist autentimist ja digitaalallkirjastamist nõudvad teenused atraktiivseks ning kasutatavaks ka piiriüleselt. Määruse põhjenduspunktis 16 väljendatakse, et vajalike turvanõuete täitmine peaks olema saavutatav erinevate tehnoloogiate abil ning kõik käesoleva regulatsiooni alusel kehtestatavad tingimused peaksid olema tehnoloogiliselt neutraalsed.

E-identimise regulatsioonist loodetakse kasu ka erasektorile ehkki kohustuslik järgimiseks on määrus üksnes liikmesriikide avaliku sektori asutustele. Seetõttu on ka mõistetav, et selleks, et e-identimise vahendite piiriülest kasutamist erasektori jaoks lihtsamaks muuta, oleks liikmesriigi pakutav autentimisvõimalus väljaspool kõnealuse liikmesriigi territooriumi asuvatele erasektori tuginevatele isikutele kättesaadav samadel tingimustel kui kõnealuses liikmesriigis asuvatele erasektori tuginevatele isikutele. Eestis on e-identimise ehk ID-tarkvara vabalt alla laetav veebikeskkonnast https://installer.id.ee/ ja tasuta kasutatav. Installeerimise käigus paigaldatakse sõltumata seadme asukohariigist arvutisse ID-kaardi haldusvahend, DigiDoc3 klient ehk digiallkirjastamise tarkvara ning ka DigiDoc krüpto ehk krüpteerimise tarkvara. Selle tulemusena on eID kasutajal võimalik tõendada oma isikut

[96] Euroopa Parlamendi ja nõukogu direktiiv 2002/21/EÜ, 7. märts 2002, elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv). – EÜT L 108, 24.4.2002. Lk 33-50.
[97] Q&A: Electronic Identification and Trust Services (eIDAS) Regulation. Brussels, 14th October 2014. Arvutivõrgus: http://europa.eu/rapid/press-release_MEMO-14-586_en.htm (18.04.2015).

elektrooniliselt, kasutada selliselt nii pankade, riigi või erinevate ettevõtete teenuseid veebi kaudu, digitaalselt allkirjastada ja krüpteerida dokumente sõltumata asukohast või ajast. Eesti ID-kaardi tarkvara lähtekood ja lähtekoodipakid on avalikud ning avaldatud veebilehel: https://github.com/open-eid/.

Tehnoloogia neutraalsuse printsiibi järgimise juures on kahtlemata põhiteguriks e-identimise süsteemide usaldusväärseks piiriüleseks vastastikuseks tunnustamiseks e-identimise süsteemide turvalisus. Seoses sellega on eIDAS määruses märgitud[98], et liikmesriigid peaksid tegema liidu tasandil koostööd e-identimise süsteemide koosvõime ja turvalisuse küsimustes, ning juhul kui e-identimise süsteemid võivad nõuda tuginevatelt isikutelt teatava riist- või tarkvara kasutamist riigi tasandil, eeldab piiriülene koosvõime, et nimetatud liikmesriigid ei kehtestaks selliseid nõudeid väljaspool tema territooriumi asuvatele tuginevatele isikutele ega nõuaks nendega seonduvate kulude katmist.

2.2.3. Andmekaitse

Euroopa Liidus on andmekaitseküsimused käesoleval perioodil erilise tähelepanu all, kuivõrd räägitakse läbi uue EL andmekaitse määruse eelnõu üle. Samas andmekaitse ning täpsemalt isikuandmete kaitse on aktuaalne ja delikaatne teemade kompleks laiemalt. Järjest enam digitaliseeruvas maailmas eskaleeruvad ka hirmud, et me oleme pidevalt kellegi jälgimise all või kas meie andmed on ikka piisavalt kaitstud[99]. Seda olulisemaks muutuvad andmekaitse küsimused ka iga innovatsiooni juures[100]. Valitsused üle maailma suunavad enam teenuseid ja toiminguid internetikeskkondadesse, et need tuua kodanikule lähemale, samas eeldavad need ligipääsemiseks riigi poolt antud eID kasutamist, mille vahel registreeritavate andmete kontroll ei ole enam isiku enese käes.[101] Läbi aegade on valitsustel olnud traditsiooniliselt

[98] EIDAS määruse põhjenduspunkt 19.
[99] Catherine Everett kirjeldab eID'ga kaasnevaid hirme Suurbritannias „Suure Venna" ühiskonna tekkimise ees oma töös „E-Identity: an isuse of trust". Computer Fraud and Security. March 2011, p. 9. Lauren Henry analüüsib oma töös „Information Privacy and Data Security" informatsiooni kaitstuse või ka privaatsuse erisusi andmekaitsest üldisemalt, kuivõrd sageli käsitletakse neid koos, mis ei ole aga õiguslikult alati põhjendatud, kuna nende eesmärgid on teine kord vastukäivad – ametiasutuste huvi kaitsta enda töödeldavaid andmeid ei ole alati kooskõlas isikute huviga kaitsta nende kohta töödeldavaid andmeid ametiasutuste poolt. Vt lähemalt L. Henry, Information Privacy and Data Security (April 29, 2015). Cardozo Law Review de Novo, 2015, Forthcoming, p.107-118. Available at SSRN: http://ssrn.com/abstract=2600495 (01.05.2015).
[100] Selleks käivitas Euroopa Komisjon suuremahulise projekti STORK, et arendada välja turvaline Euroopa eID platvorm, mis võimaldaks mistahes EL liikmesriigi e-riigi teenustele turvalist ligipääsu kõigile EL kodanikele nende oma riigi eID'ga. Vt lähemalt C. Everett "Will the e-identity STORK deliver a European baby?". Computer Fraud and Security, August 2009, p. 13.
[101] Sellega kaasnevaid ohte analüüsib Price Geraint oma töös „The benefiits and drawbacks of using

keskne roll personaalse identiteedi väljastamisel[102] läbi dokumentide, nagu sünnitunnistus, pass või juhiluba, välja andmise – ent digitaalsel ajastul on sellega kaasnevad väljakutsed mõnevõrra erinevad. Sama eID skeem võetakse enamasti standardina kasutusele ka erasektoris, nii et ka nende teenuseid saab kasutada sama digitaalse identiteedi vahendusel. Siit tuleneb olukord, kus see sama, riigi poolt väljastatav digitaalne e-identiteet muutub peamiseks vahendiks, mille kaudu isik digitaalsel ajastul üldse suhelda saab [103] [104] ja sellest johtuvalt jääb eID kandjast ning eID vahendusel tehtud toimingutest maha ka rohkem informatsiooni kui varasema mitte-digitaalse isikut tõendava dokumendi skeemi korral.

Eeltoodud põhjustel rõhutab ka eIDAS määrus andmekaitse olulisust ja peab andmete turvalist käitlemist üliolulisteks. Määruse artiklis 5 lõikes 1 nähakse selgelt ette määruse kohaldamine täielikus vastavuses isikuandmete kaitse põhimõtetega, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 95/46/EÜ[105]. Seda arvesse võttes on ette nähtud käesoleva määrusega kehtestatud vastastikuse tunnustamise põhimõtte kohaselt internetipõhise teenuse jaoks tehtava autentimise käigus töödelda üksnes ja ainult selliseid tuvastamisandmeid, mis on piisavad, asjakohased ega ületa asjaomasele teenusele internetipõhise juurdepääsu võimaldamiseks vajalikku[106]. Sama nõue kehtib ka usaldusteenuse osutajate ning järelevalveasutuste suhtes, kes peavad direktiivis 95/46/EÜ sätestatud töötlemise konfidentsiaalsuse ja turvalisuse nõuetest kinni pidama. Isikuandmete kaitse rikkumise korral pannakse määrusega järelevalveasutustele kohustus teavitada andmekaitseasutusi, kui kvalifitseeritud usaldusteenuse osutajate auditite tulemustest ilmneb, et isikuandmete kaitse eeskirju on rikutud[107]. Taoline teavitamine peab hõlmama eelkõige turvaintsidentidest teada andmist ja isikuandmetega seotud rikkumiste juhtumeid[108].

---

electronicidentities“. Information Security and Technical Report, May 2008. Vol. 13, Issue 2, p. 96-101.

[102] Paul De Hert. Identity management of the e-ID, privacy and security in Europe. A human rights view. Information Security Technical Report. May 2008, Volume 13, Issue 2, p. 72.

[103] Care Sullivan, Sophie Stalla-Bourdillon. Digital identity and French personality rights – A Way forward in recognising and protecting an individual’s rights in his/her digital identity. Computer Law and Security Review, 2015, p. 268.

[104] M. Laurent, *et al* (toim), “Digital Identity Management“, 1st Edition (2015) andmetel kasutavad 90% Interneti kasutajatest oma eID’d pääsemaks ligi just avaliku sektori e-teenustele ja e-kaubanduse teenustele ning 8% kasutavad seda e-panganduseks.

[105] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. EÜT L 281, 23.11.1995, lk 31.
Isikuandmete kaitse põhimõtte olulisust rõhutab ka eIDAS määruse põhjenduspunkt 11.

[106] Eesmärgikohasuse ja ülemäärasuse (meil ka minimaalsuse) põhimõtted on ette nähtud ning kehtivad nii hetkel kehtivas direktiivis ja isikuandmete kaitse seaduses kui on sisse kirjutatud ka tulevikus kehtima hakkavasse EL andmekaitse määrusesse.

[107] EIDAS määrus artikkel 17 lg 4 (f).

[108] Menetluskorda ja -pädevust selleks eIDAS määrus ei puuduta.

2.3. E-identimine ja e-identimise süsteemid

Käesoleva töö kontekstis on peamine määruse e-identimise süsteeme puudutav regulatsioon ning koostöö tingimused ja kord, mida tuleb liikmesriikidel või nende vastavatel asutustel järgida tulenevalt rakendusaktidega seatavatest nõuetest[109]. Antud osa puudutab määruse II peatükki ja artikleid 6-12.

Nimelt on täiesti uus olukord võrreldes varasemaga tekkinud käesoleva määruse **art 6 lg 1** kohaldamisega, mille alusel tuleb olukorras, kus ühes liikmesriigis nõutakse vastavalt siseriiklikule õigusele või haldustavale avaliku sektori asutuse osutatavale internetipõhisele teenusele juurdepääsuks e-identimist e-identimise vahendi abil ja e-autentimist, **tunnustada selles liikmesriigis teises liikmesriigis väljastatud e-identimise vahendit** kõnealuse internetipõhise teenuse **piiriüleseks autentimiseks**.

E-identimisena käsitletakse eIDAS määruse raames protsessi ehk tegevuste jada, mille käigus kasutatakse elektroonilisi isikutuvastusandmeid, mis tähistavad üheselt füüsilist või juriidilist isikut või juriidilist isikut esindavat füüsilist isikut.
Autentimine on määratletud elektroonilise protsessina, mis võimaldab füüsilise või juriidilise isiku e-identimist või elektrooniliste andmete päritolu ja tervikluse kinnitamist.
E-identimise süsteem on e-identimiseks vajalik riiklik süsteem, mille raames väljastatakse e-identimise vahendeid füüsilistele või juriidilistele isikutele või juriidilist isikut esindavatele füüsilistele isikutele.

See tähendab, et kui näiteks Eesti e-tervise keskkonda pääseb hetkel Eesti kodanikust patsient tõrgeteta ligi autentides end oma Eesti Vabariigi ID-kaardi või mobiil-IDga, et vaadata enda kohta tervise infosüsteemi saadetud terviseandmeid ja ravidokumente või määrata endale hoopis esindaja retsepti väljaostmiseks, siis sama peab saama teha kõnealuse internetipõhise teenuse puhul eIDAS määruse alusel alates 2018. aastast ka iga muu Euroopa Liidu kodanik, kellele on välja antud mõnes teises Euroopa Liidu liikmesriigis e-identimise vahend, olgu see siis Leedu, Soome või Belgia eID, kriteeriumiks on aga, et kui me nõuame teenusele

[109] EIDAS määruse juurde on vastu võetud esimene rakendusotsus (EL) 2015/296, mis käsitleb menetluskorda liikmesriikidevaheliseks koostööks e-identimise valdkonnas vastavalt eIDAS määruse artikli 12 lõikele 7 ning arutelude lõppfaasis on rakendusotsus e-identimise süsteemide usaldusväärsuse tasemete määratlemiseks ning neist teavitamiseks vastavalt eIDAS määruse artiklitele 8 ja 9 lg 1.

ligipääsemiseks e-identimist ja e-autentimist, peame selleks aktsepteerima ka teise liikmesriigi vastavat e-identimise vahendit.

Selleks sätestatakse aga edaspidi täpsemad tingimused, millele teise liikmesriigi e-identimise vahend vastama peab, et talle kohalduksid samad tingimused, kui asukohariigi eID kandjale:

1) e-identimise vahend peab olema väljastatud e-identimise süsteemi kohaselt, mis on kantud komisjoni poolt vastavalt eIDAS määruse artiklile 9 avaldatud nimekirja;
2) e-identimise vahendi usaldusväärsuse tase vastab usaldusväärsuse tasemele, mida avaliku sektori asutus nõuab kõnealusele internetipõhisele teenusele juurdepääsuks esimesena nimetatud liikmesriigis, või on sellest usaldusväärsuse tasemest kõrgem, eeldusel et selle e-identimise vahendi usaldusväärsuse tase on märkimisväärne või kõrge;
3) asjaomane avaliku sektori asutus kasutab kõnealusele internetipõhisele teenusele juurdepääsuks usaldusväärsuse taset, mille tase on märkimisväärne või kõrge.

Artikkel 9, millele viitab eelmise lõigu punkt 1, näeb teavitavale liikmesriigile ette järgnevad kohustused – teavitada:

1) liikmesriikides kasutusel oleva(te) e-identimise süsteemi(de) kirjeldusest (k.a selle usaldusväärsuse tasemest ja sellesse süsteemi kuuluvate e-identimise vahendite väljastaja(te)st),
2) järelevalvekorrast (k.a osalistest, kes e-identimise vahendit väljastab ja autentimismenetlust läbi viib),
3) teavitatud e-identimise süsteemi eest vastutava(te)st asutuse(te)st,
4) teabest ainulaadsete isikutuvastusandmete registreerimist haldava(te) üksus(t)e kohta,
5) kirjeldusest, kuidas täidetakse artikli 12 lõikes 8 osutatud rakendusaktis sätestatud nõudeid, ehk loodud koosvõime raamistiku kohaseid ühtseid tingimusi teavitatud riiklike e-identimise süsteemide osas,
6) artikli 7 punktis f osutatud autentimise kirjeldusest, ehk kuidas on tagatud internetipõhise autentimise võimalus nii, et teise liikmesriigi territooriumil asuv tuginev isik saab kinnitada elektrooniliselt saadud isikutuvastusandmeid,
7) ning teavitatud e-identimise süsteemist, autentimise või asjaomase ohustatud osa peatamisest või tühistamise korrast.

Komisjoni tuleb teavitada ilma põhjendamatu viivituseta antud loetellu kuuluvast *igast üksikust* muudatusest, olgu selleks mõne teguri muutumine e-identimise vahendi väljastamise protsessis või e-identimise süsteemi kirjelduses või muudatus isikutuvastusandmete registreerimist haldavas üksuses jmt.

Komisjon ei ole saanud käesoleva töö kirjutamise hetkel avaldada veel artikli 9 kohast nimekirja liikmesriikide e-identimise süsteemidest, kuna artikkel 9 lõike 2 kohaselt avaldab komisjon nimekirja e-identimise süsteemidest Euroopa Liidu Teatajas üks aasta pärast artikli 8 lõikes 3 ja artikli 12 lõikes 8 osutatud rakendusaktide kohaldamise alguskuupäeva[110], kuid käesoleva töö kirjutajale on kättesaadav tööversioonis artikli 8 lõige 3 rakendusakt[111], millega kavandatakse ette näha minimaalsed tehnilised kirjeldused, standardid ja menetlused, mille suhtes määratakse teavitatud e-identimise vahendite jaoks kindlaks madal, märkimisväärne või kõrge usaldusväärsuse tase. Käesoleva töö autor kasutab viidatud rakendusakti eelnõu oma töö edasises analüüsis.

Eelnevast lähtuvalt tuleb Eestil tunnustada – juhul, kui Eesti teavitab oma e-identimise skeemi(de)st – vastavalt teiste riikide eID süsteeme juhul, kui vastava teise liikmesriigi e-identimise vahendi usaldusväärsuse tase on võrdväärsel tasemel Eesti eID-le määratud tasemega või – juhul, kui Eesti ei teavita oma e-identimise skeemidest või jätab teavitamata mõnest kasutatavast skeemist – aktsepteerida teiste liikmesriikide eID-sid, mille usaldusväärsuse tase vastab usaldusväärsuse tasemele, mida meie avaliku sektori asutus nõuab kõnealusele internetipõhisele teenusele juurdepääsuks, või on sellest kõrgem, eeldusel et selle teise liikmesriigi e-identimise vahendi usaldusväärsuse tase on märkimisväärne või kõrge.

Praegusel ajal on Eesti võimeline ise teiste riikide eID-de suhtes hinnangut andma iga konkreetse riigi kohta ühekaupa ja eraldi. Teiste riikide sertide hindamisel kasutatakse hetkel Majandus- ja Kommunikatsiooniministeeriumi riigi infosüsteemide osakonna (RISO) poolt väljatöötatud "Teiste riikide eID hindamise põhimõtted[112]" metoodikat. Selle alusel on positiivne hinnang antud käesoleva töö kirjutamise hetkel Sertifitseerimisregistri andmetele

[110] Mis on määruse kohaselt ette nähtud vastu võtta hiljemalt 18. septembri 2015. a.
[111] Riiklike ekspertide jaoks komisjoni portaali CIRCABC üles aletud 14. aprill 2015 seisuga. Asub Lisas 1.
[112] Arvutivõrgus: http://www.riso.ee/et/koosvoime/identiteet/teiste-riikide-serdid.html (22.03.2015).
Riigi infosüsteemide osakonna andmete kohaselt ei ole Eestis otseselt nõudeid avaliku sektori teenuste jaoks sertifikaatide kvaliteedile kehtestatud, küll aga on Eestis kehtiv digitaalallkirja seadus ja isikut tõendavate dokumentide seadus, mille alusel Eesti ID-kaarti väljastatakse ning hinnangu andmisel on lähtutud just põhimõttest kontrollida, kas teise riigi sertifitseerimisteenuse osutaja ja sertifikaatide turvalisus on võrdväärsel tasemel Eesti ID-kaardi omaga.

tuginedes[113] Eesti poolt seitsme riigi: Belgia, Hispaania, Itaalia, Leedu, Portugali, Sloveenia ning Soome eID-de sertifikaatidele, mis tähendab, et nende riikide sertifitseerimisteenuse osutajad ja sertifikaatide turvalisus on juba praegu loetud võrdväärsel tasemel olevaks Eesti ID-kaardi omaga. Samas ei ole käesolevalt kasutatav metoodika lähemas perspektiivis enam täielikult sobilik, kuna see ei baseeru eIDAS määruse regulatsioonil ning lähtub elektroonilise allkirja direktiivi 1999/93/EÜ lisades 1 ja 2 toodud baasnõuetest sertifitseerimisteenuse osutajatele ja nende poolt väljastatavatele sertifikaatidele. Liikmesriikide seadusandlustes on varieeruvusi ja seega pole üks-ühene kõrvutamine alati võimalik. Lähtuda tuleb üldisematest, standardiseeritud ning hästi defineeritud kriteeriumitest, mille alusel hinnanguid anda. Hindamiskriteeriumid tuleb eIDAS määrusesse jäetud ülemineku aja jooksul üle vaadata ning viia kooskõlla eIDAS määruse ja selle alusel vastuvõetavate rakendusaktide nõuetega. Artikli 6 kohane vastastikuse tunnustamise nõue jõustub ning muutub seeläbi kohustuslikuks alates määruse artiklites 8 lõikes 3 ja 12 lõikes 8 ettenähtud rakendusaktide kohaldamise alguskuupäevast kolme aasta möödumisest[114].

Tänaste hinnangute alusteks on RISO andmetel[115] kaks Euroopas teadaolevalt üldist metoodikat, mis kirjeldavad eID turvaklasse: 1) Euroopa Komisjoni IDABC poolt tellitud töö: „Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms[116]“ ja 2) De Norske Veritas valideerimisteenuse poolt kasutatav skaala, kuid mõlemad on tänaseks paljuski aegunud ja asendatud juba komisjoni poolt finantseeritud Large Scale Pilot projekti STORK[117] (*Secure idenTity acrOss boRders linKed*) tulemustega. STORK eesmärgiks oli luua n.ö Euroopa eID platvorm, mis võimaldaks mistahes EL liikmesriigi e-riigi teenustele ligipääsu kõigile EL kodanikele nende oma riigi eIDga[118]. Hetkel on käimas STORK projekti teine etapp: STORK 2.0, mille raames piloteeritakse riiklike eID-de piiriülest rakendust läbi nelja[119] rahvusvahelise pilootprojekti. STORK-le viitab mh nii eIDAS määrus kui artikli 8 lõike 3 kohane komisjoni rakendusotsuse kavand. Kuid mõlemad viitavad ka ISO 29115 standardile[120], kus mõlemis on käsitletud

[113] Arvutivõrgus: https://sr.riik.ee/et/usaldusnimekiri/TeisedRiigid.html (16.04.2015).
[114] Määruse artikkel 52 lg 2 punkt c.
Vabatahtlik tunnustamine on võimalik käesoleva aasta sügisest vastavalt määruse artikkel 52 lõikele 4.
[115] Arvutivõrgus: http://www.riso.ee/et/koosvoime/identiteet/teiste-riikide-serdid.html (08.04.2015).
[116] Arvutivõrgus: http://ec.europa.eu/idabc/en/document/6484.html (08.04.2015).
[117] Arvutivõrgus: https://www.eid-stork.eu/dmdocuments/public/mapping.pdf (08.04.2015).
[118] Arvutivõrgus: https://www.eid-stork.eu/ (08.04.2015).
[119] Pilootprojektideks on 1) *eLearning and Academic Qualifications Pilot*, 2) *eBanking Pilot*, 3) *Public Services for Business Pilot*, 4) *eHealth Pilot*. Eesti osaleb neist kolmanda pilootprojekti töös läbi Registrite ja Infosüsteemide Keskuse.
[120] Vt eIDAS määrus põhjenduspunkt 16 ja käesoleva töö Lisa 1 (lk 84).

hindamismetoodikaid, seega on need teeviidad parimate praktikate valimiseks, kuid ei määrus ega kavand baseeru ise otseselt kummalgi.

Selleks, et riiklikult kasutusel olevatele e-identimise vahenditele usaldusväärsuse taset eIDAS määrusele vastavalt määrata, tuleb liikmesriigil aga esmalt komisjoni artikkel 9 kohaselt teavitada[121]. Liikmesriigil on käesoleva määruse kohaselt tegelikkuses vabadus otsustada[122], kas enda e-identimise süsteemidest, ja kui neid on kasutusel enam kui üks, siis millistest, komisjoni teavitada. Määrus seda ühegi artikliga *expressis verbis* küll ei väljenda, kuid regulatsioonile eelnevas põhjenduspunktis 13 märgitakse, et liikmesriikidel on võimalus valida, kas teavitada komisjoni kõikidest riigisiseselt vähemalt avalikele internetipõhistele teenustele juurdepääsuks kasutatavatest e-identimise süsteemidest, teha seda ainult mõne süsteemi puhul või seda üldse mitte teha. Liikmesriikidel peaks jääma vabadus kasutada või juurutada e-identimise vahendeid juurdepääsuks internetipõhistele teenustele.

Ehkki esmapilgul võib näida, et määruse regulatsioon on suunatud e-identimise süsteemide vastastikuse tunnustamise, usaldusväärsuse tasemete määramise ning koosvõime ja koostöö regulatsiooni osas üksnes 'teavitavatele' liikmesriikidele, kuna usaldusväärsuse tasemeid näeb määrus ette määrata artikli 8 kohaselt üksnes artikli 9 lõike 1 kohaselt teavitava liikmesriigi e-identimise süsteemi(de)le ja vastastikust hindamist tuleb läbida vaid teavitatud e-identimise süsteemide puhul, siis määruse tegelik ja sügavam eesmärk on juhtida erisusteta kõiki liikmesriike Euroopa Liidu majandust ergutavale koostööle, kasutades selleks eIDAS määruse mõtte ja sätete keerukamat tõlgendusmehhanismi, mida käesolev töö järgnevalt läbi tunnustamise ja vastastikuse hindamise mehhanismide avab.

Artikkel 6 eIDAS määruses, mis näeb ette liikmesriikide eID-de vastastikuse tunnustamise kohustuse, sätestab ühtlasi ka tingimused, millele vastavalt antud kohustust on nõutud täita. Selles on nähtud, et vastastikuse tunnustamise kohustus kohaldub tingimusel, et:

1) tolle (teise) liikmesriigi e-identimise vahend, mida esimene liikmesriik tunnustama peab, on väljastatud e-identimise süsteemi kohaselt, mis on kantud komisjoni poolt vastavalt artiklile 9 avaldatud nimekirja. Artikli 9 lõikes 2 nimetatud nimekiri käsitleb

[121] Vt käesoleva magistritöö punkt 2.3.1.
[122] Kui määrusega oleks liikmesriikidele ette nähtud kohustus kõikidest riiklikest eID süsteemidest komisjoni teavitada ning neile määrusega kehtestatavad tasemed määrata, oleks see potentsiaalselt ohtu seadnud EL lepingu artikkel 5 kohase subsidiaarsuse ja proportsionaalsuse põhimõtte (käsitletud käesoleva pöö alapeatükis 2.1.) järgimise.

e-identimise süsteeme, millest on teavitatud vastavalt sama artikli lõikele üks. Sellest tulenevalt peab nimetatud (teine) liikmesriik, kes soovib, et tema e-identimise vahendit esimeses liikmesriigis tunnustataks võrdselt esimeses liikmesriigis kasutusel olema e-identimise vahendiga, olema oma e-identimise süsteemist komisjoni teavitanud;

2) tolle (teise) liikmesriigi e-identimise vahendi usaldusväärsuse tase vastab usaldusväärsuse tasemele, mida avaliku sektori asutus nõuab kõnealusele internetipõhisele teenusele juurdepääsuks esimesena nimetatud liikmesriigis, või on sellest usaldusväärsuse tasemest kõrgem, eeldusel et selle (teise) liikmesriigi e-identimise vahendi usaldusväärsuse tase on märkimisväärne või kõrge. Usaldusväärsuse tase (madal, märkimisväärne ja/või kõrge) määratakse määruse artikli 8 lõike 1 kohaselt vastavalt e-identimise süsteemidele, millest on teavitatud artikli 9 lõike 1 kohaselt;

3) asjaomane (esimese) liikmesriigi avaliku sektori asutus kasutab kõnealusele internetipõhisele teenusele juurdepääsuks usaldusväärsuse taset, mille tase on märkimisväärne või kõrge. Käesolev tingimus ei viita küll ühelegi teavitamis-kohustuse nõudele ja on teada, et usaldusväärsuse taseme määramiseks, millele vastavat taset asjaomane avaliku sektori asutus kõnealusele internetipõhisele teenusele juurdepääsuks kasutada võib, saab käia üksnes e-identimise vahendi kohta ja seda määratakse määruse artikkel 8 (e-identimise süsteemide usaldusväärsuse tasemed) järgi, mis näeb ette taseme määramise e-identimise süsteemidele, millest on teavitatud artikli 9 lõike 1 kohaselt, seega tuleb antud juhul viimast tingimust tõlgendada kui olukorda, millisel juhul, kui liikmesriigi avaliku sektori asutus võimaldab kõnealusele internetipõhisele teenusele juurdepääsu riikliku e-identimise vahendiga (olenemata sellest, kas vastava riigi e-identimise vahendist on teavitatud artikli 9 lõikele 1 kohaselt või mitte), mille tase vastab usaldusväärsuse tasemele märkimisväärne või kõrge, tuleb seda võimaldada ka teise liikmesriigi võrdväärse teavitatud e-identimise vahendiga. Antud kriteeriumi sõnastus ei ole ehk kõige õnnestunum, kuna jätab tõlgendaja sisustada, mil moel asutus internetipõhisele teenusele usaldusväärsuse taset määrab, kuivõrd sellist protsessi määrus lähemalt ei kirjelda, kuid määruse üldisest lähenemisviisist usaldusväärsuse tasemele tuletades võib sellest siiski üle saada.

Eelkirjeldatud tingimused ei ole konkureerivad ja üksteist välistavad, vaid peavad olema täidetud vastastikuse tunnustamise eelduseks kõik üheaegselt.

Eelnevale lisandub täiendus artikkel 6 lõikest 2 – nimelt loob see võimaluse madalal tasemel e-identimise vahendi tunnustamiseks vabatahtlikuse alusel, kuna e-identimise vahendit, mis on väljastatud komisjoni poolt vastavalt artiklile 9 avaldatud nimekirjas oleva süsteemi kohaselt ning mille usaldusväärsuse tase on madal, *võivad* avaliku sektori asutused tunnustada nende asutuste osutatavate internetipõhiste teenuste piiriülese autentimise eesmärgil, kuid selleks ei tulene neile kohustust, nagu lõikes 1 nimetatud märkimisväärse ja kõrge tasemega identimisvahendite korral.

Seega kokkuvõtlikult järeldub eelnevast, et liikmesriikidel on vaba voli otsustada kas oma e-identimise süsteemidest teavitada või jätta teavitamata. Teavitava liikmesriigi puhul on üheselt selge, et kus teavitatud on kõigist antud liikmesriigis kasutusel olevatest riiklikest e-identimise süsteemidest, millega riiklikele e-teenustele ligi pääseb, rakendub nõue tunnustada samaväärsele või kõrgemale tasemele vastava teise liikmesriigi eID-d ning võimaldada sellega sama ligipääs, v.a taseme *madal* korral, millal võib seda teha vabatahtlikuse alusel. Teavitamata jätva või teatud juhul osalise teavitamise otsustuse korral (juhul, kui liikmesriigis on kasutusel enam kui üks e-identimise süsteem), peab liikmesriik arvestama võimalikkusega, et kui tema avalik sektor võimaldab internetipõhisele teenusele ligipääsu oma riigi kodanike eID-dega, tuleb samale teenusele võimaldada juurdepääsu ka teise liikmesriigi e-identimise vahendiga, mis on samale tasemele vastav või sellest kõrgem, eeldusel et selle (teise) liikmesriigi e-identimise vahendi usaldusväärsuse tase on märkimisväärne või kõrge. See eeldab, et tolle teise liikmesriigi e-identimise vahend on läbinud teavitamisprotsessi vastavalt määruse artikli 9 lõikele 1 ja kantud artikkel 9 lõikes 2 nimetatud nimekirja. Teavitamisprotsessi käsitleb lähemalt järgnev alapeatükk.

Kirjeldatust tekib aga huvitav paradigma – nimelt, kui (esimene) liikmesriik ei ole enda e-identimise süsteemidest või mõnest kasutatavast teavitanud, ei tulene talle ka otsest kohustust oma e-identimise vahenditele usaldusväärsuse tasemeid määrata. Määruse artikkel 8 lõige 1 ütleb üheselt, et usaldusväärsuse tase *madal*, *märkimisväärne* ja/või *kõrge* määratakse e-identimise süsteemi raames, millest on teavitatud artikli 9 lõike 1 kohaselt, väljastatud e-identimise vahenditele. Seega, kuidas teada, millistele eeldustele vastab teise liikmesriigi avaliku sektori e-teenus, kes ei ole oma süsteemidest teavitanud või seda kasutatakse mõne

riikliku e-identimise süsteemi poolt, millest ei ole teavitatud. Sellele küsimusele vastab autor käesoleva töö alapeatükis 2.3.2.2[123].

Silmas tuleb aga pidada seejuures siiski ka määruse andmiseni viinud käesoleva töö esimeses osas kirjeldatud Euroopa Liidu püüdlust pääseda läbi eIDASe regulatsiooni digitaalse turu killustatusest ja jõuda täielikult integreeritud digitaalse ühtse turuni[124], mis lihtsustaks internetipõhiste teenuste piiriülest kasutamist. Eraldi pöörab määrus erilist tähelepanu turvalise e-identimise ja e-autentimise hõlbustamisele, mistõttu on vastu võetud iseseisev koostöövorm ja kord, nn koosvõime raamistik[125]. Samas ei kohusta eIDAS määrus siiski kedagi e-identimise vahendeid kasutama või neid looma, kui neid kasutusel ei ole.

2.3.1. E-identimise süsteemist teavitamine

E-identimise süsteemist saab liikmesriik teavitada määruse artikli 9 lõikele 1 vastavalt juhul, kui selleks on täidetud 8 eeltingimust[126].

1. Esmalt – kui e-identimise süsteemi kuuluv e-identimise vahend on väljastatud vastavalt ühele kolmest kriteeriumist: see peab olema väljastatud kas teavitava liikmesriigi enda poolt, teavitava liikmesriigi antud volituse alusel või siis sõltumatult teavitavast liikmesriigist, kuid see liikmesriik tunnustab antud e-identimise vahendit. Esimesel juhul annab liikmesriik e-identimise vahendeid ise välja (Eestis annab isikutunnistuse, digitaalse isikutunnistuse, mobiil-ID, elamisloakaardi ja e-residendi digitaalse isikutunnistuse välja Politsei- ja Piirivalveamet[127]), teisel juhul on liikmesriik delegeerinud eID väljaandmise enda käest ära ning volitanud selleks kedagi kolmandat (võib olla ka erasektorit) ning kolmandal juhul toimub eID väljastamine liikmesriigist sõltumatult, kuid antud liikmesriik tunnustab selliselt väljaantud vahendit ning seda on võimalik kasutada sama riigi digitaalses asjaajamises isiku veebipõhisel autentimisel.

2. Teiseks – e-identimise süsteemi kuuluvat e-identimise vahendit saab kasutada juurdepääsuks liikmesriigi vähemalt ühele teenusele, mida osutab selle avaliku sektori asutus ning mis eeldab teavitavas liikmesriigis e-identimist – näiteks nagu Eestis maksude deklareerimine. Praxise 2013. a läbiviidud uuringu andmetel on Maksu- ja Tolliameti e-

[123] Leheküljel 50.
[124] EIDAS määruse põhjenduspunktid 4 ja 5.
[125] Komisjoni rakendusotsus (EL) 2015/296, ELT L 53, 24.02.2015, lk 14-20.
[126] EIDAS määrus atikkel 7.
[127] Vastavalt ITDS §-d 15 lg 4 ja 20^{11} lg 1.

keskkonna kasutamine Eestis kasutatavatest e-teenustest kõige populaarsem – järgnevad digiretsept, avalike teenuste eest maksmise võimalus ja riigilõivu tasumine Internetipanga kaudu ning veebilehte www.eesti.ee külastamine, kuhu on kokkuvõtlikult ühte kontaktpunkti koondatud kümneid Eesti riigis pakutavaid e-teenuseid[128]. Kõik eeltoodud teenused eeldavad neis isiku kohta käivatele andmetele ligipääsemiseks aga ka e-identimist, seega kui neile saab ligi Eesti e-identimise süsteemi kuuluva e-identimise vahendiga, on vastav kriteerium meie puhul täidetud.

3. Selleks, et e-identimise süsteemist teavitada, peab e-identimise süsteem ja selle kohaselt väljastatud e-identimise vahend vastama ka vähemalt ühe usaldusväärsuse taseme (madal, märkimisväärne või kõrge) nõuetele, mis on sätestatud määruse artikli 8 lõikes 3 osutatud rakendusaktis. Vastava rakendusakti kavand sisutab usaldusväärsuse tasemete *madal*, *märkimisväärne* ja *kõrge* määramise täpsemad kriteeriumid, mida on järgnevalt käesoleva töö alapeatükis 2.3.2. toodule vastavalt põhjalikumalt analüüsitud.

4. Teavitav liikmesriik peab tagama, et ainulaadsed kõnealust isikut tähistavad isikutuvastusandmed omistatakse määruse artikli 3 punktis 1 osutatud füüsilisele või juriidilisele isikule sellesse süsteemi kuuluva e-identimise vahendi väljastamisel[129] kooskõlas tehniliste kirjelduste, standardite ja menetlustega, mis on artikli 8 lõikes 3 osutatud rakendusaktis ette nähtud asjakohase usaldusväärsuse taseme jaoks. See tähendab, et isikule eID väljaandmisel peab olema järgitud viidatud rakendusakti kohaselt vastava taseme kõiki elemente[130] koostoimes konkreetsele tasemele vastava kõnealust isikut ainulaadselt tähistavate isikutuvastusandmete omistamiskriteeriumidega[131]. Nendeks on *madala* taseme puhul nõue, et e-identimise vahend peab kasutama vähemalt üht autentimise tegurit ning et selline e-identimise vahend on konstrueeritud nii, et tema puhul võib eeldada, et seda saab kasutada ainult siis, kui see on vaid isiku valduses, kellele see kuulub; *märkimisväärse* taseme puhul peab e-identimise vahend kasutama vähemalt kahte autentimise tegurit kahest erinevast autentimise tegurite kategooriast ning et selline e-identimise vahend on konstrueeritud nii, et võib mõistlikult eeldada, et seda saab kasutada ainult siis, kui see on isiku valduses, kellele see kuulub; *kõrge* taseme puhul peab e-identimise vahend kasutama vähemalt kahte autentimise tegurit kahest erinevast autentimise tegurite kategooriast ning kaitsma e-

[128] Kalvet, T., Tiits, M., Hinsberg, H. E-teenuste kasutamise tulemuslikkus ja mõju. Uuringu aruanne. Balti Uuringute Instituut ja Poliitikauuringute Keskus Praxis. Tallinn, 2013, lk 16. Arvutivõrgus: http://www.praxis.ee/fileadmin/tarmo/Projektid/Valitsemine_ja_kodanike%C3%BChiskond/E-teenuste_kasutamise_tulemuslikkus_ja_moju.pdf (10.04.2015).

[129] Art 3 p 1: „e-identimine" on protsess, mille käigus kasutatakse elektroonilisi isikutuvastusandmeid, mis tähistavad üheselt füüsilist või juriidilist isikut või juriidilist isikut esindavat füüsilist isikut.

[130] Vt rakendusotsuse eelnõu, Lisas 1.

[131] Rakendusotsuse eelnõu punkt 2.2.1, lk 93.

identimise vahendit kopeerimise ja rikkumise eest. Selline e-identimise vahend on konstrueeritud nii, et olles isiku käes, kellele ta kuulub, on see usaldusväärselt kaitstud kolmandate isikute kasutuse eest.[132] Konstruktsiooni "kellele [eID vahend] kuulub" tuleks mõista siin mitte kui valdajat asjaõiguse mõttes – ja isikut, kellele kuulub tegelik võim asja üle[133] – vaid pigem kui isikut, kellel on seadusest tulenev õigus asja vallata, kasutada ja käsutada – konkreetset isikut, kelle nimele vastav e-identimise vahend väljaantud on – omanikku. Eesti riigis väljaantavad eID-d võivad kanda endas digitaalset isiku tuvastamist võimaldavat informatsiooni, sealhulgas digitaalset tuvastamist võimaldavat krüptograafilist võtit ning sellele vastavat sertifikaati ja digitaalset allkirjastamist võimaldavat informatsiooni, sealhulgas digitaalset allkirjastamist võimaldavat krüptograafilist võtit ning sellele vastavat sertifikaati ning teisi digitaalseid andmeid. Eestis väljaantavad eID-d on kõigil juhtudel varustatud kahe sertifikaadiga[134], võimaldades nii isikutuvastust, andmete krüpteerimist kui digitaalallkirjastamist, nende andmekandja on ette nähtud olema piisava mahu ja suutlikkusega, et kindlustada sellele kantud andmete terviklikkus, autentsus ja konfidentsiaalsus[135] ning eID kasutamine elektroonilises keskkonnas nõuab tema omanikult personaalsete turvakoodide[136] teadmist. Eestis kasutusel olevate eID-de väljaandmine on Politsei- ja Piirivalveameti kontrolli all (mobiil-ID puhul väljastab vastava kiipkaardi isikule küll mobiilioperaator, kus ITDS § 20^4 lg 7 alusel on mobiilioperaator kohustatud kooskõlastama mobiil-ID vormis digitaalse isikutunnistuse tehnilise lahenduse enne selle kasutusele võtmist Riigi Infosüsteemi Ametiga, kes küsib selleks menetluse käigus Politsei- ja Piirivalveameti ja sertifitseerimisteenuse osutaja seisukohta[137], kuid sertifikaadid, millega internetipõhise teenuse puhul isiku autentimine toimub, väljastatakse teenuse aktiviseerimisel Politsei- ja Piirivalveameti kodulehel[138]), mistõttu tuleb pidada riigi kontrolli all väljaantavat süsteemi kolmandate osapoolte eID-de manipulatsioonide eest ka piisavalt kaitstuks.

---

[132] Rakendusotsuse eelnõu punkt 2.2.1, lk 93.

[133] Asjaõigusseadus § 33 lg 1.

[134] Isikutunnistuse vormi ja tehnilise kirjelduse ning isikutunnistusele kantavate andmete loetelu kehtestamine ja isikutunnistusele kantavate digitaalsete andmete kehtivusaja määramine, § 5 lg 1 (RT I, 17.12.2010, 2 – RT I, 09.08.2011, 1); Digitaalse isikutunnistuse vormi, tehnilise kirjelduse ja digitaalsele isikutunnistusele kantavate andmete loetelu kehtestamine, § 5 lg 1 (RT I 2010, 61, 422 – RT I, 28.11.2014, 11); Eesti Vabariigi välja antava elamisloakaardi vormi ja tehnilise kirjelduse ning elamisloakaardile kantavate andmete loetelu kehtestamine ja elamisloakaardile kantavate digitaalsete andmete kehtivusaja määramine, § 5 lg 1 (RT I 17.12.2010, 3 – RT I, 14.10.2014, 3); mobiil-ID puhul ITDS § 20^4 lg 1 (RT I 1999, 25, 365 – RT I, 23.03.2015, 1).

[135] Siseministri 12.08.2010 määrus nr 36 "Digitaalseks isiku tõendamiseks ettenähtud dokumendi andmekandja tehnilised nõuded", punkt 1. (RT I 2010, 66,495 – RT I, 23.12.2010, 5)

[136] PIN1, PIN2 või PUK koodi, mis on mõeldud vastavalt isikutuvastuseks, digitaalallkirjastamiseks ja lukustunud PIN-koodide lahtitegemiseks.

[137] ITDS muudatus RT I, 21.03.2014, 2 – jõust. 01.05.2014.

[138] Arvutivõrgus: https://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/mobiil-id/ (13.04.2015)

5. Sellesse süsteemi kuuluvat e-identimise vahendit väljastav osaline tagab e-identimise vahendi omistamise määruse artikli 7 punktis d osutatud isikule kooskõlas tehniliste kirjelduste, standardite ja menetlustega, mis on artikli 8 lõikes 3 osutatud rakendusaktis ette nähtud asjakohase usaldusväärsuse taseme jaoks. See tähendab, et isikule eID väljastamisel peab olema järgitud viidatud rakendusakti kohaselt vastava taseme kõiki elemente koostoimes konkreetsele tasemele vastava väljaandmisprotseduuri spetsifitseeritud kriteeriumidega[139]. Nendeks on *madala* taseme puhul nõue, et peale e-identimise vahendi väljaandmist valitakse selle kättetoimetamiseks viis, mille puhul võib eeldada, et see tagab vahendi jõudmise üksnes isikuni, kellele ta mõeldud on; *märkimisväärse* taseme puhul peab e-identimise vahendi väljaandmise järel olema eID kättetoimetamiseks valitud viis, mis võimaldab mõistlikult eeldada, et see jõuab üksnes isiku valdusse, kellele eID kuulub; *kõrge* taseme puhul nähakse ette, et aktiviseerimisprotsess[140] ise juba tagab/kinnitab, et vastav e-identimise vahend toimetati või anti üle vaid selle isiku valdusse, kellele eID kuulub.[141] Eesti Vabariigis kehtiva isikut tõendavate dokumentide seaduse alusel antakse isikut tõendavaid dokumente välja üksnes antud seaduses sätestatud alustel[142] ning üldjuhul tuleb isikul dokumendi kättesaamiseks ilmuda isiklikult dokumendi väljastaja asukohta, et dokumendi väljastaja saaks dokumendi väljastamisel tuvastada taotleja isiku. Dokumendi kättesaamise kohta annab dokumendi taotleja allkirja.[143] Taoline protseduur täidab ära määruse artikkel 8 lõike 3 alusel antava rakendusakti *kõrgemale* tasemele vastava kriteeriumide kirjelduse nõuded.

6. Teavitav liikmesriik tagab internetipõhise autentimise võimaluse nii, et teise liikmesriigi territooriumil asuv tuginev isik saab kinnitada elektrooniliselt saadud isikutuvastusandmeid. Tuginev isik määruse mõistes on füüsiline või juriidiline isik, kes tugineb e-identimisele või usaldusteenusele. Määruse artikkel 8 lõige 3 punkti c kohaselt on antud tingimused seatud sõltuvusse vastavast usaldusväärsuse kvaliteedi tasemest, mille konkreetsed elemendid on läbirääkimiste all rakendusotsuse eelnõu punktis 2.3.1[144]:

Madal	- isikut tuvastava informatsiooni väljaandmisele eelneb usaldusväärne eID vahendi ja selle kehtivuse kinnitamine; - seal, kus isikut identifitseerivaid andmeid hoitakse autentimise

[139] Rakendusotsuse eelnõu punkt 2.2.2, lk 93. Vt Lisa 1.
[140] Meie mõistes dokumendi väljaandmise (ITDS § 10) ja väljastamise protsess (ITDS § 12^1 ja § 12^2).
[141] EIDAS määruse artikkel 8 lõike 3 kohase rakendusakti eelnõu (käesoleva töö Lisas nr 1), p 2.2.2, lk 93.
[142] ITDS § 10 lg 1.
[143] *Ibid*., § 12^1 lg 2.
[144] Käesoleva töö Lisa nr 1, lk 94-95.

	mehhanismi osana, peab see informatsioon olema kaitstud võimalike andmekadude või kompromiteerimise eest, sh võimaliku võrguvälise (i.k *offline*) analüüsi eest; - autentimismehhanism tagab vajalikud turvakontrollid eID vahendite kinnitamisel selliselt, et algteadmisest edasiarendatud potentsiaaliga ründajale on muudetud ülimalt ebatõenäoliseks autentimissüsteemi õõnestada arvamise, pealkuulamise, taastamise või kommunikatsiooni manipulatsioonide teel.
Märkimisväärne	Samad tingimused, mis taseme *madala* puhul ning lisanduvad: - ID informatsiooni väljaandmisele eelneb usaldusväärne eID vahendi ja selle kehtivuse kinnitamine läbi dünaamilise autentimisprotsessi[145]; - autentimismehhanism tagab vajalikud turvakontrollid eID vahendite kinnitamisel selliselt, et mõõduka või keskmise potentsiaaliga ründajale on muudetud ülimalt ebatõenäoliseks arvamise, pealkuulamise, taastamise või kommunikatsiooni manipulatsioonide teel autentimissüsteemi õõnestada.
Kõrge	Samad tingimused, mis taseme *märkimisväärne* puhul ning lisandub: - autentimismehhanism tagab vajalikud turvakontrollid eID vahendite kinnitamisel selliselt, et ka kõrge potentsiaaliga ründajale on muudetud ülimalt ebatõenäoliseks arvamise, pealkuulamise, taastamise või kommunikatsiooni manipulatsioonide teel autentimissüsteemi õõnestada.

Eestis on eID-de autentimislahendus eraldiseisev e-identimisvahendi väljaandmisprotseduurist ning väljaandjast. Autentimislahendus on väljatöötatud AS Sertifitseerimiskeskuse poolt AS TRÜB Baltic partnerina ning Sertifitseerimiskeskus hoolitseb rakenduste edasise arendamise, leviku ja halduse eest. Veebipõhine autentimislahendus toimib selliselt, et Eestis kasutatava eID autentsuse kontroll on konfigureeritud toimuma veebiserveris rakendustele nähtamatult – veebiserver nõuab isikult, kes ennast veebis autentida soovib, sertifikaati (seda nõutakse isiku veebibrauserilt, kuidas konkreetne brauser seda omakorda isikult küsib, sõltub konkreetsest brauserist) – ning saades brauserilt sertifikaadi, kontrollib veebiserver, et see

[145] *Dünaamilise autentimisprotsessi* mõiste on defineeritud kui protsess, milles kasutatakse krüptograafiat või muid meetodeid, et luua unikaalne autentifikaator (i.k. *authenticator*), mis muutuks küsija/autentija ja verifitseerija/kontrollija vahel iga autentimise korral;
(Vt eIDAS määruse artikkel 8 lõike 3 kohase rakendusakti eelnõu punk 1(3), lk 88).

sertifikaat oleks allkirjastatud AS Sertifitseerimiskeskuse poolt ega oleks kantud AS Sertifitseerimiskeskuse poolt väljastatud sertifikaatide tühistusnimekirjadesse[146]. Nende sammude läbimisel võimaldatakse isikule ligipääs vastavasse kaitstud keskkonda. Sertifitseerimiskeskuse (SK) infosüsteemid logivad kõiki SK kinnitusvõtmete elutsükli etappe ja kasutamist, kõiki klientide võtmete elutsükli etappe, kõiki turvasündmusi, nagu kasutajate autoriseerimised või edutud autoriseerimise katsed ning kõiki eriõigustega süsteemikasutajate tegevusi. Infotehnoloogiliste ja organisatsiooniliste vahenditega on tagatud logide muutmatus, säilimine ja konfidentsiaalsus. Samuti kasutab SK standarditele vastavaid infoturbe-lahendusi[147], mis tagavad isiklike võtmete, aktiveerimiskoodide, pääsukoodide (näiteks PIN-ide) ja muu turvakriitilise informatsiooni logis mittesalvestumise. Spetsiaalne turvalise logi süsteem tagab krüptograafiliste meetoditega logikirjete ajalise järjestuse ja tervikluse[148], mis koostoimes peaksid tagama kõrgemal tasemel meie autentimismehhanismi kaitstuse võimalike pahatahtlike manipulatsioonide või sekkumist eest.

7. Vähemalt kuus kuud enne määruse artikli 9 lõike 1 kohast teavitamist esitab teavitav liikmesriik teistele liikmesriikidele artikli 12 lõikest 5 tuleneva kohustuse täitmiseks, mis näeb ette teavitavate liikmesriikide vahelise koostöö tegemise kohustuse koosvõimet ja turvalisust käsitleva teabe osas, selle süsteemi kirjelduse artikli 12 lõikes 7 osutatud rakendusaktidega kehtestatud menetluskorra kohaselt. Rakendusotsuse (EL) 2015/296 kohane menetluskord näeb ette, et teabe, kogemuste ja heade tavade ning koosvõimet ja turvalisust käsitlevat teavet tuleb vahetada ühtsete kontaktpunktide kaudu ning nõutud asjakohane teave tuleb esitada põhjendamatu viivituseta[149]. 2006. aasta detsembris vastu võetud Euroopa Parlamendi ja nõukogu direktiiviga nr 2006/123/EÜ[150] on nõutud liikmesriikidelt juba ühtsete kontaktpunktide loomist, tagamaks, et kõiki teenuste osutamise valdkonnas tegutsemise alustamise ja selles valdkonnas tegutsemisega seotud toiminguid ja formaalsusi oleks lihtne teha eemalt elektrooniliste vahendite abil sobiva ühtse kontaktpunkti kaudu ja koos asjaomaste ametiasutustega. Eesti ühtseks kontaktpunktiks sai toona määratud riigiportaal www.eesti.ee[151] – paljud ühtsete kontaktpunktide kaudu kättesaadavad internetipõhised teenused eeldavad ka täna juba e-identimist, e-autentimist või digiallkirja. Riigiportaali

[146] Tühistusnimekirjad on failid, milles on info kõigi hetkel tühistatud või peatatud sertifikaatide kohta. Arvutivõrgus: https://sk.ee/repositoorium/CRL/CRL (13.04.2015).
[147] Nt ISO 13335, ISO 13569.
[148] Sertifitseerimiskeskuse sertifitseerimispõhimõtted (*Certification Practice Statement*), versioon 2.5. Peatükid 4-6. Arvutivõrgus: https://www.sk.ee/repositoorium/CPS/ (13.04.2015).
[149] Komisjoni rakendusotsus (EL) 2015/296, artikkel 6.
[150] Euroopa Parlamendi ja nõukogu 12. detsembri 2006. aasta direktiiv 2006/123/EÜ teenuste kohta siseturul (ELT L 376, 27.12.2006, lk 36).
[151] Arvutivõrgus: http://ec.europa.eu/internal_market/eu-go/index_en.htm#ee (11.04.2015).

eesti.ee haldab Riigi Infosüsteemi Amet (RIA), kes koordineerib Eesti riigi infosüsteemi arendamist ning haldamist, korraldab infoturbega seotud tegevusi ja käsitleb Eesti arvutivõrkudes toimuvaid turvaintsidente[152], siis oleks eIDAS määruse kontekstis samuti loogiline ning mõttekas liigse killustatuse vältimiseks, kui direktiivi nr 2006/123/EÜ alusel Eesti ühtseks kontaktpunktiks määratud keskkonda haldav ning riigi infosüsteemi arendamist, haldamist ja infoturvet korraldav asutus RIA määrataks üksusena ühtseks kontaktpunktiks ka rakendusotsuse (EL) 2015/296 mõttes. Antud tingimustel võib käesoleva nõude lugeda tinglikult Eesti puhul eeltäidetuks, kuni astutakse tegelikud sammud meil kasutusel olevatest e-identimise süsteemidest teavitamiseks.

8. E-identimise süsteem peab vastama ka määruse artikli 12 lõikes 8 osutatud rakendusaktis sätestatud nõuetele. Antud rakendusakt koosvõime raamistiku kohta võetakse komisjon poolt vastu hiljemalt 18. septembriks 2015 artikkel 12 lõikes 3 sätestatud kriteeriumide kohaselt ja liikmesriikidevahelise koostöö tulemusi arvesse võttes.

Selleks, et liikmesriik oma e-identimise süsteemi(de)st teavitada saaks, peavad olema valimatult täidetud määruse artikkel 9 lõike 1 *kõik* eeltingimused. Seega saab eeltoodust hetkel vaid osaliselt järeldada, et Eesti e-identimise süsteemid võiksid vastata teavitamise kriteeriumidele – väita saab seda kindlalt vaid eeltingimuste osas, mis eksisteerivad sõltumatult komisjoni ettevalmistatavate rakendusaktide vastuvõtmisest ning nende kohaselt täidame juba täna kriteeriume 1, 2, 6 ning 7. Eeltingimused nr 3, 4, 5 ja 8 eeldavad määruse artiklite 8 lõike 3 ja 12 lõike 8 kohaste rakendusaktide vastuvõtmist.

2.3.2. E-identimise süsteemide usaldusväärsuse tasemed

Selleks, et liikmesriigil tekiks võimalus endi kasutusel olevatest e-identimise süsteemidest teavitada, tuleb esmalt hinnata nende vastavust komisjoni poolt määruse artiklis 8 toodud usaldusväärsuse tasemetele ja artikkel 8 lõige 3 alusel vastuvõetava rakendusaktiga kehtestatavatele tehnilistele kirjeldustele, standarditele ja menetlustele ning seejärel paigutada iga e-identimise vahend sobivalt nõuetele vastavasse e-identimise süsteemi. Järgnevalt analüüsib autor ja käsitleb minimaalseid tehnilisi kirjeldusi ja menetlusi rakendusakti enim eriarvamusi ja vaidlusi põhjustanud peatükkidest, need on 2.1-2.3[153], olles osa moodustatavast

[152] RIA tegevusvaldkond ja põhiülesanded on määratud Riigi Infosüsteemide Ameti põhimääruse 2. peatükis, s.o §-d 7-9. Arvutivõrgus: https://www.riigiteataja.ee/akt/128042011001?leiaKehtiv (11.04.2015).
[153] Vt Lisa 1, käesoleva töö lk 88-95.

eID turvatasemest, mis on Eesti e-identimise süsteemi(de) kvalifitseerimisel määrava tähtsusega.

Riiklike eID-de usaldusväärsuse tasemete kindlaks määramiseks tuleb uurida lähemalt komisjoni väljatöötatavas rakendusotsuses kirjeldatud kriteeriume. Vastavalt käesoleva töö peatükis 1.3.3.1. toodule on käsitlemist leidnud, et Eesti Vabariigis on kasutusel viis erinevat e-identimise vahendit: isikutunnistus, digitaalne isikutunnistus, mobiil-ID, elamisloakaart ja e-residendi digitaalne isikutunnistus. Usaldusväärsuse tasemetele vastavust tuleb hinnata neist igaühe puhul eraldi.

Komisjon pakub oma rakendusakti eelnõus välja füüsiliste isikute identiteedi kontrollimise ja kinnitamiseks[154] järgneva kvalifitseerimismudeli:

Madal	Kõik all-loetletud elemendid peavad olema täidetud üheaegselt: 1. Võib mõistlikult eeldada, et isikul on olemas tema kohta väidetud isikusamasust tõendavad riiklikult tunnustatud tõendid. 2. Tõendid tunduvad olevat kehtivad (i.k. *valid*). 3. Autoriteetse(te) allika(te)[155] andme(te)l on väidetav identiteet teadaolevalt olemas/eksisteerib ega ole teada selle surmast. 4. Taotleja identifitseeritakse kasutades autoriteetsest allikast saadud teavet.
Märkimisväärne	Täidetud peab olema tase *madal*, pluss üks järgnevatest alternatiividest: 1. On tõendanud, et isikul on olemas tema isikusamasust tõendavad riiklikult tunnustatud tõendid ja need on vastavalt autoriteetse allika andmetele kontrollitud ning need määravad, et identiteet on ehtne või kehtiv; või 2. Kui liikmesriigis, milles dokument on välja antud, esitatakse registreerimise protsessi käigus sama liikmesriigi riiklikult väljastatud identifitseeriv dokument, ning see tundub siduvat dokumendi selle esitanud isikuga ning see näib ehtne, seejuures kontrollitakse ega pole teatatud selle kadumisest, vargusest,

[154] Vt Lisa 1, p 2.1.2, lk 89-91.

[155] 'Autoriteetne allikas' on defineeritud kui *ükskõik milline allikas, millele võib tugineda õigete/tõeste andmete, informatsiooni ja/või dokumentide esitamisel, mis võivad [isiku] identiteeti tõendada*. Rakendusotsuse eelnõu, vt Lisast 1, lk 88.

	peatamisest või kehtetuks tunnistamisest, võib sellist dokumenti pidada iseseisvalt autoriteetseks allikaks; või 3. Liikmesriigis, kus on [üksuse poolt] mõneks muuks otstarbeks kui elektroonilise identifitseerimise vahendite käibele laskmiseks varem kasutatud protseduure, mis pakuvad täpselt samaväärset tagatist vastavatele usaldusväärsuse tasemetele, mis on sätestatud käesoleva rakendusotsuse punktiga 2.1.2, ei pea too elektroonilise identifitseerimise vahendit väljastav asutus kordama neid samu varem läbiviidud protseduure, kui on tagatud, et sellega võrdne tagatis on antud vastavushindamisasutuse poolt, millele viitab EÜ määruse nr 765/2008/EÜ artikel 2 punktis 13[156] või teise samaväärse [asutuse] poolt; või 4. Seal, kus elektroonilise identifitseerimise vahendid on välja antud, v.a uuendamise või asendamise eesmärgil, teavitatud elektroonilise identifitseerimise vahendite alusel, millel on sama või kõrgem usaldusväärsuse tase, ei olda kohustatud registreerimise protsessi kordama. Seal, kus aluseks olevad elektroonilise identifitseerimise vahendid ei ole teavitatud, peab samaväärne või kõrgem usaldusväärsuse tase olema kinnitatud vastavushindamisasutuse poolt, millele viitab EÜ määruse nr 765/2008/EÜ artikel 2 punktis 13 või teise samaväärse [asutuse] poolt.
Kõrge	Täidetud peab olema üks kahest allolevast alternatiivist: 1. Tase *märkimisväärne,* pluss üks alternatiividest (a, b või c): **a.** Kus on kindlaks tehtud, et isikul, kes taotleb väidetavat identiteeti, on juba olemas riiklikult tunnustatud foto või biomeetrilisete andmetega identifitseerimise tõend/biomeetriliste andmetega isikutunnistus, kontrollitakse tõendit/isikutunnistust vastu autoriteetset allikat, et kindaks teha, et see on ehtne ja kehtiv; - ja taotleja on identifitseeritud kui see, kellena ta end väidab olevat, läbi tolle isiku ühe või mitme füüsilise karakteristiku võrdluse

[156] EÜ määruse nr 765/2008 artikkel 2 p 13: „vastavushindamisasutus" – asutus, mis teostab vastavushindamist, sealhulgas kalibreerimist, katsetamist, sertifitseerimist ja kontrolli.

	usaldusväärse allika poolt esitatud tõendite vastu; või **b.** Sama, mis punkt 3 *märkimisväärse* taseme juures, aga vastab tasemele *kõrge* koos järgnevaga: - on kindlaks tehtud, et varem läbitud protseduuri tulemused on kehtivad; või **c.** Sama, mis punkt 4 märkimisväärse taseme juures, pluss kontrollitakse, et ükski varem välja antud elektroonilise identifitseerimise vahend, mida võib kasutada [elektroonilise isikutunnistuse] väljaandmise alusena, ei ole teadmata kadunud, varastatud, peatatud või kehtetuks tunnistatud. 2. Kus taotleja ei esita ühtegi tunnustatud fotot või biomeetriliste andmetega isikutunnistust, kasutatakse samu menetlusprotseduure, mida kasutatakse riiklikul tasandil, et selline tunnustatud foto või biomeetrilise identifitseerimise tõend/biomeetriliste andmetega isikutunnistus saada.

E-identimise usaldusväärsuse kvaliteedi tasemele madal, märkimisväärne ja kõrge vastavad elemendid füüsilise isiku puhul.

Antud kriteeriumid on liikmesriikide ekspertidega korduvate kohtumiste raames läbi vaieldud, kuid arutelud kestavad veel 2015.a mai kuu lõpuni, mil antud rakendusotsus komitees hääletusele pannakse. Komisjon on leidnud küll, et juuresolevas on ekspertide panust arvesse võetud, mistõttu ei nähta põhjust olemasolevas märkimisväärsete muudatuste tegemiseks[157], kuid nähtavasti tuleb arvestada siiski teatavate modifikatsioonivõimalustega viimases, vastuvõetavas versioonis. Kasutan aga juuresolevat määratlust käesoleva töö edasises analüüsis, et hinnata, millised potentsiaalsed riskid või väljakutsed meid Eesti eID-de usaldusväärsustasemete kategoriseerimisel ees oodata võivad.

Põhimõtteliselt võib iga e-identimise vahend kvalifitseeruda vastava määratluse eri tasemele või moodustada tervikus ühe e-identimise süsteemi. Viimases olukorras peavad need eri e-identimise vahendid mahtuma rakendusotsuses ettekirjutatavate tasemete ühe määratluse kõigi kriteeriumide tõlgendusruumi. Eestil on kahtlemata ambitsioon kvalifitseerida enda e-identimise vahendid usaldusväärsuse tasemele *kõrge* vastavaks. Seda võib ette näha esmalt turvalisuse kaalutlustel, et hoida ära teiste liikmesriikide poolt teavitatud aga *kõrgest* madalama usaldusväärsuse tasemega vahendite lubamist ligi meie riiklikele andmekogudele

[157] Rakendusakti eelnõu, vt Lisa 1, lk 84.

ning elektroonilistele teenustele võrdväärselt meie eID kasutajatega – madalama usaldusväärsuse tasemega kvalifikatsiooni on mõnevõrra kergem täita, nende kasutajaid on eelduslikult rohkem ning nende kasutuses olevate e-identimise vahendite turvalisuse tase ei pruugi vastata Eesti ID-kaardiga võrdväärsetele standarditele. Teiseks, kui Eesti e-identimise vahendi tase kvalifitseerub usaldusväärsuse tasemele *kõrge* vastavaks, pääsevad meie eID omanikud ligi kõikide teiste liikmesriikide avaliku sektori e-teenustele. Juhul, kui see oleks madalam (nt märkimisväärne), ei kaasneks sellega teistele *kõrgema* tasemega ligipääsetavatele teenustele juurdepääsu – seega on kaalukausil selgelt ka meie kodanike ning teiste Eesti eIDde kasutajate võimalikud piiriülesed kasud. Ning viimaks ei ole vähemoluline ka asjaolu, et Eestil on kõrgetasemelise IT-riigi mainekuvand – meie IT-lahendusi tuntakse Silicon Valley'st kuni Singapurini. Eesti e-riigi arenguindeks EGDI (i.k *e-Government Development Index*) on 2014. aasta ÜRO e-valitsuste uuringus kvalifitseeritud üheks "väga kõrge" EGDI tasemega riikidest maailmas[158], olles "väga kõrge" EGDI arenguindeksiga riikide topis sealjuures üleilmselt 15ndal[159] ja Euroopa kontekstis 8ndal[160] kohal. Meil on tulemused ja kuvand, mida tasub hoida ning edasi arendada. Seega on Eesti riigi üldistes huvides, mitte anda oma standardites järele ja lubada riiklike e-teenuste kasutamisel oma süsteemidesse muid kui kõige kõrgemate usaldusväärsuse kriteeriumidele vastavaid e-identimise süsteeme, vaid tagada selleks volitatud vahendite väljaandmis- ja turvalisus-protseduuride piisav usaldusväärsuse kontroll.

Lähtudes üksnes eIDAS määruse artikli 8 lõikest 2 võiksid Eesti e-identimise süsteemide usaldusväärsuse tasemed nii isikutunnistuse (ID-kaardi), mobiil-ID, digitaalse isikutunnistuse, elamisloakaardi kui e-residendi digitaalse isikutunnistuse puhul olla kvalifitseeritavad usaldusväärsuse tasemele "kõrge"[161] vastavaks. Vahetegu määruse kontekstis esitatud kvalifikatsioonitaseme “kõrge” ja "märkimisväärne" vahel seisneb nimelt eesmärgis esimese puhul *hoida ära isikuandmete väärkasutamist või muutmist*, kui teise kohaselt püütakse *märkimisväärselt vähendada* isikuandmete väärkasutamise või muutmise ohtu. Kuna aga määruse vastuvõtmisega läks 2014. aastal eesseisvate Euroopa Parlamendi valimistega kiireks

[158] United Nations E-Government Survey 2014. E-Government for the Future We Want. Table 1.2. Countries grouped by EGDI in alphabetical order, lk 17.

[159] *Ibid*., tabel 1.1 "World e-government leaders (Very High EGDI) in 2014", lk 15.
Võrreldes 2012. aastaga on Eesti ülemaailmses võrdlustabelis tõusnud 5 koha võrra.

[160] *Ibid*., tabel 1.7 "Top 20 countries in Europe", lk 31.

[161] Art 8 lg 2 (c): kõrge usaldusväärsuse tase osutab e-identimise süsteemi kuuluvale e-identimise vahendile, mis on isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks kõrgema usaldusväärsuse tasemega kui märkimisväärse usaldusväärsuse tasemega e-identimise vahend ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on hoida ära isikuandmete väärkasutamist või muutmist.

– eIDAS-t oli tolle koosseisuga selleks hetkeks menetletud juba pea kolm aastat[162] ning Euroopa digitaalse tegevuskava eesmärk e-identimise ja e-autentimise vastastikuseks tunnustamiseks kogu Euroopa Liidus vajas tulemusi – ei jõutud kõikides protseduurides üksmeelele ning kõiki detaile ka lõpuni läbi arutatud, kuid seepärast ei saanud määrust järgneva parlamendi koosseisu ootele jätta. Seetõttu on mitmed lahti kirjutamata protseduurid reguleeritud määruse asemel hoopis rakendusaktidega, mis määruse norme täiendavad. See ei ole iseenesest problemaatiline, kui antud viisil on keerukad valdkonnad leidnud põhjalikumat läbimõtlemist, mis on määrava tähtsusega iga regulatsiooni eeltöös. Samas ei jõutud eIDAS artikkel 8 lõikes 2 nimetatud usaldusväärsuse tasemete määramise protseduure määruses lähemalt reguleerida ning nendele vastavuse kontrolliks tuleb pöörduda artikkel 8 lõikele 3 vastava rakendusakti (hetkel eelnõu[163]) poole. Eeltoodust järelduvalt tuleb Eesti eID-de tegelike usaldusväärsuse tasemete määramiseks lisaks määruse artikkel 8 lõikes 2 toodule analüüsida, kas meie viis e-identimise vahendit kvalifitseeruvad ka rakendusotsuses kavandatava kohaselt usaldusväärsuse tasemega *kõrge* ettenähtavaid elemente täitma.

2.3.2.1. Autoriteetne allikas

EIDAS määruse artikkel 8 lõike 3 alusel kavandatava rakendusotsuse eelnõu kasutab e-identimise süsteemide usaldusväärsuse elementide määratlemisel mitmel pool mõistet "autoriteetne allikas". Antud definitsiooni kohaselt võib olla autoriteetne allikas ükskõik milline allikas, millele saab tugineda õigete/tõeste andmete, informatsiooni ja/või dokumentide esitamisel, mis võivad [isiku] identiteeti tõendada[164]. Nimetatud definitsioon on äärmiselt lai – sinna alla võivad kuuluda nii dokumendid, andmed kui informatsioon ükskõik millisest allikast, mida võib lugeda vähegi usaldusväärseks. Ei ole öeldud, et sellel peab olema seos riikliku asutuse, üksuse või protsessiga. Näiteks võib "ükskõik milline allikas", millele tugineda õigete/tõeste andmete, informatsiooni ja/või dokumentide esitamisel, mis võivad [isiku] identiteeti tõendada, olla nii teise riigi isikut tõendavat dokumenti väljaandev asutus kui hüpoteesi mõttes ka prügikoritusfirma, kes on võimeline näitama, et too isik tasub iga kuu nende teenusarveid, pangaülekande tegija on panga poolt verifitseeritud, nii et järelikult on isik (ja tema kantav identiteet) olemas.

[162] Euroopa Komisjon tegi eIDAS määruse ettepaneku teatavaks 4ndal juunil 2012 ning pärast mitmeid muudatusi, 24ndal veebruaril 2014 saavutati poliitiline kokkulepe Euroopa Parlamendi liikmete, Euroopa Komisjoni ja Euroopa Nõukogu vahel.
[163] Vt käesoleva töö Lisa 1.
[164] *Ibid*., lk 88.

Tegelikkuses jääb määratlus mõistagi liialt laiaks ja suuresti liikmesriikide endi ja nende viljeletava praktika kujundada, et seda piisavalt täpselt sisustada. Hetkel ei ole võimalik antud definitsiooni järgi üheselt ja selgelt määratleda, kes või mis saab täita autoriteetse allika rolli. Kui antud sõnastust lõppeva komitoloogiamenetluse raames täpsemaks kokku ei lepita (näiteks kitsendades seda vastava liikmesriigi isikut tõendavat dokumendi väljaandva asutuse/üksuse või isiku sündi/surma registreeriva asutuse/üksusega), võiks kaaluda Eesti-sisese määratluse kokkuleppimist, millisel juhul oleks alati selge, mis on vastava rakendusotsuse definitsiooni raames meie jaoks 'autoriteetne allikas' ning millele Eesti riigis tuginetakse. Selleks võiks olla isiku olemasolu kindlakstegemiseks Eesti rahvastikuregister kui riigi põhiregister, kuhu kantakse andmed Eesti kodaniku, Eestis elukoha registreerinud Euroopa Liidu, Euroopa Majanduspiirkonna liikmesriigi ja Šveitsi Konföderatsiooni kodaniku ning Eestis elamisloa või elamisõiguse saanud välismaalase kohta[165]. Rahvastikuregistrisse kantakse andmed ka isiku surma kohta[166]. Samuti võib dokumendi kehtivuse kontrollimisel olla selleks isikut tõendavate dokumentide andmekogu[167], kuhu kantakse mh andmed ka mitteresidentidest e-residendi digitaalse isikutunnistuse taotleja kohta (küll aga mitte nende isikute surma kohta). E-residentide andmeid rahvastikuregistris ei registreerita[168].

2.3.2.2. Isikutuvastusprotsess e-identimise süsteemi määramisel

Eestis kasutusel olev **elektrooniline isikutunnistus** on ITDS mõttes isikut tõendav dokument, mis on välja antud riigiasutuse poolt ning kuhu on kantud kasutaja nimi ja sünniaeg või isikukood ning foto või näokujutis ja allkiri või allkirjakujutis. Dokumendi väljaandmisel on ette nähtud protseduur[169], mille kohaselt kontrollib taotlemisel dokumendi väljaandja dokumendi taotleja isikusamasust kehtiva dokumendi ja isikut tõendavate dokumentide andmekogusse kantud isiku tuvastamise andmete vastu. Dokumendi kasutaja isikusamasuse kontrollimisel tehakse dokumendi kasutaja isik kindlaks dokumenti kantud andmete ning isiku võrdlemise teel, ning seejuures võib isikusamasuse kontrollimisel võrrelda dokumendi kasutajalt võetud biomeetrilisi andmeid dokumenti kantud biomeetriliste andmete vastu.[170]

[165] Rahvastikuregistri seadus § 4.
[166] *Ibid*., § 21 lg 1 p 14.
[167] Vabariigi Valitsuse 03.07.2008. a vastuvõetud määrus nr 109 "Isikut tõendavate dokumentide andmekogu pidamise põhimäärus". RT I 2008, 31, 195 – RT I, 28.11.2014, 11.
[168] Rahvastikuregistri seadus, § 4.
[169] ITDS § 11^1.
[170] *Ibid*., § 18^1 lg 1.

Juhul, kui dokumenti taotlevale isikule ei ole eelnevalt ITDS-s sätestatud isikut tõendavat dokumenti välja antud, tuvastab Politsei- ja Piirivalveamet dokumendi taotleja isiku ning kannab selle kohta isiku tuvastamise andmed isikut tõendavate dokumentide andmekogusse[171]. Dokumendi kättesaamiseks peab isik isiklikult ilmuma dokumendi väljastaja asukohta, kus dokumendi väljastaja kontrollib väljastamisel veelkord dokumendi taotleja isikusamasust ning kättesaamise kohta annab dokumendi taotleja väljastajal allkirja. Kui alla 15-aastase või piiratud teovõimega dokumendi taotleja taotluse esitab seaduslik esindaja, kontrollitakse niisamuti seadusliku esindaja isikusamasust või tuvastatakse tema isik ITDS-i § 2 lõikes 2 nimetatud kehtiva isikut tõendava dokumendi või sama seaduse § 4 lõikes 1 sätestatud nõuetele vastava kehtiva isikut tõendava dokumendi alusel. Seadusliku esindaja isikusamasust võidakse kontrollida või tema isik tuvastada ka välisriigi poolt väljaantud kehtiva reisidokumendi alusel.[172]

Seega toimub Eestis isikutunnistuse, millega saab isik ühtlasi kaasa riiklikult tunnustatud elektroonilise identiteedi (eID), väljastamisel taotleja riiklikul tasemel isikusamasuse kontroll vähemalt kahel korral – esmalt isikusamasuse kontrolli käigus dokumendi taotlemisel kehtiva dokumendi ja isikut tõendavate dokumentide andmekogusse kantud isiku tuvastamise andmete vastu ning dokumendi väljastamisel silmast-silma kohtumise läbi, millise juures tuleb kättesaamise toimingul anda isikul selle kohta ka allkiri. Seega vastab antud protseduur rakendusotsuse *kõrge* taseme kvalifitseerimispunktis 1a. toodud elementidele, mis näevad ette dokumendi ja isikusamasuse kontrolli vastu autoriteetset allikat ning taotleja esitatava isikut tõendava dokumendi ehtsuses ja kehtivuses veendumise. Samuti täidab ta ära eeltingimuse tasemelt *märkimisväärne* (antud juhul nii *märkimisväärse* punkti 1 kui 2), mis on juuresolevate kriteeriumide puhul tasemele *kõrge* vastamise eelduseks. Kuid selleks, et täita tervikuna antud *kõrge* taseme määratlust, peavad täidetud olema ka kõik taseme *madal* elemendid (need on taseme *märkimisväärne* täitmise eelduseks). Sellest lähtuvalt peaksid täidetud olema ka nõuded, et: 1) oleks võimalik mõistlikult eeldada, et isikul on olemas tema kohta väidetud isikusamasust tõendavad riiklikult tunnustatud tõendid; 2) need tõendid tunduvad olevat kehtivad; 3) autoriteetse allika andmetel on väidetav identiteet teadaolevalt olemas/eksisteerib ega ole teada selle surmast ning 4) taotleja identifitseeritakse kasutades autoriteetsest allikast saadavat teavet. Viimati nimetatutest on punktid 1, 2 ja 4 eelneva

[171] Vabariigi Valitsuse 03.07.2008. a vastuvõetud määrus nr 109 “Isikut tõendavate dokumentide andmekogu pidamise põhimäärus”. RT I 2008, 31, 195 – RT I, 28.11.2014, 11.
[172] Siseministri 10.07.2009 määrus nr 25 "Dokumendi taotleja isiku tuvastamise ja isikusamasuse kontrollimise kord". RTL 2009, 57, 836 – RT I, 23.12.2010, 5.

isikusamasuse ja dokumendi kontrolli raames täidetud elemendid, kuid punktis 3 nimetatud kontroll, et väidetav identiteet on autoriteetse allika andmetel olemas (ehk selline isik on olemas – kontroll Rahvastikuregistrist) ning puuduvad teated tema surmast (samuti kontroll Rahvastikuregistrist), oleksid sellisel juhul Eestis läbitavad samaaegselt isikusamasuse kotnrolliga, kuivõrd kui isikusamasust kontrollitakse, ei oleks järgnevad menetlustoimingud võimalikud, kui riikliku andmekogu andmetel ilmseks, et nimetatud isik on surnud või tunnistatud surnuks. Seega võib nimetatud eeldusi kogumis hinnates leida, et elektroonilise isikutunnistuse väljaandmise menetlusprotsess täidab ära rakendusotsuse eelnõu p 2.1.2 kohased *kõrgele* tasemele vastavad isikusamasuse tõendamise ja kontrolli menetluse elemendid.

Samas lasub Genfi konventsiooniga[173] ühinenud riikidel kohustus väljastada oma territooriumil viibivale ja kehtiva reisidokumendita pagulasele isikutunnistus[174]. Eesti on pagulasseisundi konventsiooniga ühinenud 19.02.1997[175], seega täidetakse ka meil konventsiooni artiklist 27 tulenevat kohustust. Eestis väljaantav isikutunnistus kannab endas alati aga isiku elektroonilist identimist võimaldavat sertifikaati: isikutunistuse kontaktkiibile kantakse isiku digitaalset tuvastamist võimaldav sertifikaat, digitaalset allkirjastamist võimaldav sertifikaat ning nendes sertifikaatides sisalduvatele avalikele võtmetele üheselt vastavad isiklikud võtmed ja andmefail[176] - seega on Eestis väljaantav isikutunnistus alati ka eos e-identimise vahendiks. Pagulasseisundiga taotleja puhul ei pruugi olla võimalik tema isikusamasust kehtiva dokumendi vastu kontrollida ning ebatõenäoline oleks ka isiku tuvastamine vastu isikut tõendavate dokumentide andmekogusse kantud andmeid. Seetõttu sobib antud olukorra lahendamiseks rakendusotsustuse kvalifitseerimispunktis 2 ette nähtud alternatiiv *kõrge* usaldusväärsuse tasemega e-identimise vahendi isikutuvastsusmenetlusele juhuks, kui isikul ei ole enda kohta esitada ühtki foto või biomeetriliste andmetega dokumenti.

[173] 27.07.1951.a vastuvõetud pagulasseisundi konventsioon. Avaldatud RT II 1997, 6, 26.
[174] *Ibid*., artikkel 27.
[175] Pagulasseisundi konventsiooni ja 31. jaanuari 1967. aasta pagulasseisundi protokolliga ühinemise seadus. RT II 1997, 6, 26.
[176] Vabariigi Valitsuse 09.12.2010 määrus nr 169 "Isikutunnistuse vormi ja tehnilise kirjelduse ning isikutunnistusele kantavate andmete loetelu kehtestamine ja isikutunnistusele kantavate digitaalsete andmete kehtivusaja määramine" § 5 lg 1. RT I, 17.12.2010, 2 – RT I, 09.08.2011, 1.

Samaselt eelnevaga on ITDS mõttes Eestis isikut tõendavavaks dokumendiks, millele on ühtlasi isiku tuvastamist ja digitaalallkirjastamist võimaldavad sertifikaadid[177] – Eestis väljaantav **elamisloakaart**. Elamisloakaardi väljaandmise protseduur[178] näeb ette elamisloakaardi väljastamise 1) Eestis püsivalt elavale kolmanda riigi kodanikule, kellel on kehtiv elamisluba või elamisõigus, 2) kolmanda riigi kodanikule, kellel on Eestis viibimiseks rahvusvahelise sõjalise koostöö seaduse alusel antud luba või 3) välismaalase, kellel on Eestis viibimiseks rahvusvahelise sõjalise koostöö seaduse alusel antud luba, ülalpeetavale isikule, kui ülalpeetav isik on kolmanda riigi kodanik ja viibib Eestis koos nimetatud välismaalasega. Käesoleva lõigu punkti 1 alla kuuluvad ka varjupaigataotleja ja ajutise kaitse alusel elamisloa taotlejad, kellele võidakse väljastada elamisluba välismaalasele rahvusvahelise kaitse andmise seaduse[179] § 41 kohaselt. Selline elamisluba vormistatakse elamisloakaardile[180].

Tulenevalt ITDS § 11^4 lõike 1 ja 2 nõudest tuleb biomeetriliste andmetega dokumendi väljaandmiseks esitada isikul taotlus isikult või seadusliku esindaja kaudu dokumendi väljaandmiseks pädevale asutusele, pöördudes selleks dokumendi väljaandmiseks pädevasse asutusse. Teatud erijuhtudel, saab tähtajalist elamisõigust või alalist elamisõigust omav kolmanda riigi kodanik, pikaajalise elaniku elamisluba omav kolmanda riigi kodanik või kui ta on alla 15-aastane või piiratud teovõimega täisealine isik, siis tema seaduslik esindaja esitada taotluse elamisloakaardi väljaandmiseks isiklikult Eesti konsulaarametnikule, kes edastab selle taotleja isikusamasuse kontrollimise ja biomeetriliste andmete võtmise järel läbivaatamiseks Politsei- ja Piirivalveametile[181]. Järgneb isikutuvastusmenetlus sarnaselt isikutunnistuse puhul kirjeldatuga. Seega võib elamisloakaardi isikutuvastusmenetluse lugeda vastavaks rakendusotsuse *kõrge* taseme kvalifitseerimispunktis 1a. toodud elementidele, mis näevad ette isikusamasuse ja dokumendi kehtivuse kontrolli vastu autoriteetset allikat (milleks võib olla ka isikut tõendav dokument ise[182]), kuid hetkel kohustab *kõrge* taseme eelduseks langeva (läbi *märkimisväärse* taseme täitmise nõude) *madala* taseme punkti 3 sõnastus[183] isikusamasuse kontrolli käigus veenduma, et väidetav identiteet on autoriteetse allika andmetel olemas (ehk selline isik on olemas) ning puuduvad teated tema surmast. Kuivõrd autoriteetse allika definitsioon on üsna lai ning võimaldab autoriteetseks allikaks pidada ka

[177] ITDS § 34^2 lg 1.
[178] *Ibid*., § 34^1 lg 1.
[179] Välismaalasele rahvusvahelise kaitse andmise seadus. RT I 2006, 2, 3 - RT I, 23.03.2015, 1.
[180] *Ibid*., § 47.
[181] ITDS § 11^4 lõiked vastavalt 5^1, 5^2 ja 5^3.
[182] Autoriteetse allika analüüsiks vaata punkti 2.3.2.1.
[183] Vt käesoleva magistritöö lk 45-46.

isikut tõendavat dokumenti ennast, saab lugeda esimese eeltingimuse täidetuks, kuid punkti teine pool, mis nõuab kontrolli teostamist, et selline isik ei ole surnud, ei ole Eestis resideeruva välismaalase puhul ühegi andmekogu vastu võimalik. Teadaolevalt ei ole Euroopas olemas tänasel päeval üht üleeuroopalist või ühendatud riiklike surmade registrit – liikmesriigiti on ka surmade registreerimine lahendatud erinevalt – Eestis kantakse isiku surma või surnuks tunnistamise andmed rahvastikuregistrisse, kuid see ei ole ilmtingimata nii kõigis liikmesriikides. Seega tuleks antud kriteeriumi jõustamise korral teostada eelkirjeldatud päringud isiku suhtes tema elukoha riiki. Euroopas on mõeldav, et pärides vastu teise liikmesriigi vastavat isikutunnistust väljaandvat asutust, saab sellele vastuse, kuid kolmandate riikide puhul ei garanteeri miski neilt kinnituse, ümberlükkamise või üldse mingisugusegi vastuse saamist. Leidub riike, kel puudub sündide ja surmade registreerimiseks üleriigiline andmekogu ja nende andmete väljaselgitamiseks tuleb pöörduda kas kohalike omavalitsusüksuste või kirikuraamatute poole. Üks tõlgendusviis antud olukorrast ülesaamiseks võiks olla, et isiku mitte surnud olemise fakt tuvastatakse vastu isiku enda poolt esitatavat kehtivat isikut tõendavat dokumenti – autoriteetset andmekandjat ennast – kuivõrd ka isikut tõendavat dokumenti on lubatud autoriteetseks allikaks pidada, siis kui sellele talletatud foto ja/või biomeetrilised andmed langevad kokku dokumendi esitanud isiku väljanägemisega, võiks isiku lugeda vastu autoriteetset allikat sel viisil kontrollituks. Paraku ei ole selline tõlgendusalternatiiv piisavalt kandev ja usaldusväärne, et välistada olukorrad, kus võib olla kasutatud teise sarnase väljanägemisega isiku fotoga isikut tõendavat dokumenti. Seega, kui me soovime, et Eestis väljaantav elamisloakaart kvalifitseeruks antud tingimustel kõrgema usaldusväärsuskategooria alla, tuleks käesolevast kriteeriumist püüda jätkuvate läbirääkimiste käigus välja manööverdada ja sõnastada antud säte ringi selliselt, et kontrollida tuleb vaid isiku eksisteerimist (*the claimed identity is known to exist*), kuna sellisel juhul tõendab isiku eksisteerimist juba tema nimele välja antud isikut tõendav dokument.

Digitaalne isikutunnistus on oma sisus korduvdokument, kuivõrd seda antakse välja Eesti kodanikule ning välismaalasele, kellele on varem välja antud isikutunnistus või elamisloakaart või kes taotleb isikutunnistust või elamisloakaarti samaaegselt digitaalse isikutunnistusega[184]. Erinevalt kahe eelneva dokumendiga puudub digitaalsel isikutunnistusel isiku foto või näokujutis ning seda ei saa kasutada isiku tuvastamiseks füüsilises maailmas, vaid see annab isikule võimaluse end identifitseerida digitaalses keskkonnas. Digitaalse isikutunnistuse taotlemisel kehtib isikutuvastamise protseduur samaselt isikutunnistuse taotlemisele.

[184] ITDS § 20^1 lg 2.

Digitaalset isikutunnistust on võimalik välja anda ka **mobiil-ID** vormis, mille digitaalset tuvastamist võimaldav sertifikaat ja digitaalset allkirjastamist võimaldav sertifikaat on seotud mobiiltelefoni SIM-kaardiga[185]. Ka mobiil-ID puhul on tegemist n.ö korduvdokumendiga, kuna selle taotlemiseks peab isikul olema eelnevalt väljastatud kehtiv isikut tõendav dokument. Erinevalt eelkirjeldatud dokumentidest, mis endas eID-d kannavad, ei saa mobiil-ID vormis digitaalset isikutunnistust taotleda esindaja kaudu ning seda ei väljastata esindajale. Mobiil-ID vormis digitaalse isikutunnistuse kättesaamiseks ei pea isik küll isiklikult ilmuma dokumendi väljastaja asukohta (milleks Eesti kontekstis on PPA esindus), vaid vajab juba eelnevat elektroonilist isikutuvastamist võimaldavat dokumenti, millel oleksid kehtivad sertifikaadid ning mobiil-ID teenust võimaldavat SIM-kaarti. Mobiil-ID aktiveeritakse elektrooniliselt PPA kodulehel kasutades selleks digitaalset isikutuvastamist – kehtiv ITDS võimaldab dokumendi kasutaja isikusamasuse kontrollimist ka digitaalselt, millisel juhul tehakse seda isikule väljastatud kehtiva e-identimise vahendi digitaalset tuvastamist võimaldava sertifikaadi kaudu[186]. Selleks on omakorda vajalik omada kas elektroonilist isikutunnistust, elamisloakaarti või digitaalset isikutunnistust koos PIN koodide ja kehtivate sertifikaatidega. Kuna nii digitaalse isikutunnistuse (digi-ID) kui mobiil-ID puhul on isikusamasuse kontrollil järgitud rakendusotsuse eelnõus kavandatava *kõrge* taseme kvalifitseerimispunkti 1a. elemente nii nagu need on kirjeldatud isikutunnistuse väljaandmise menetluse juures, ja punkti 2 puhul on tegemist punkti 1 suhtes alternatiivse alusega, võib nimetatud eID-de väljaandmise meetmed lugeda rakendusotsuse punkti 2.1.2 *kõrgele* tasemele vastavaks.

E-residendi digitaalse isikutunnistuse (e-residendid digi-ID) näol on tegemist üleeuroopaliselt aga ka -maailmselt üsna ainulaadse identimise vormiga. E-residendi digi-ID on eelkirjeldatud kodanikele ja residentidele väljaantavatest digitaalsetest isikutunnistustest erinev nii kontseptuaalses kui õiguslikus mõttes. Sellest lähtuvalt on e-residendi digi-ID menetlusprotsessis olulisi erisusi. E-residendi digi-ID on kodaniku ja residendi digi-ID-ga identne üksnes tehnilises ja funktsionaalses mõttes, kuna kasutab dokumendi väljaandmiseks sama tehnoloogilist lahendust, kuid menetluslikus ja protseduraalses mõttes kohalduvad sellele hoopis teised reeglid.

[185] ITDS § 20^4 lg 1.
[186] *Ibid*., § 18^1 lg 2.

E-residendi digi-ID on digitaalne dokument, mida antakse välja mitteresidentidele. Seda ei saa taotleda kodanik ega välismaalane, kellele on varem välja antud Eesti isikutunnistus või elamisloakaart. Seetõttu on e-residendi digitaalset isikutunnistuse väljaandmist taotlev isik erinevalt residentidest kohustatud tõendama või põhistama e-residendi digitaalse isikutunnistuse väljaandmise aluseks olevaid asjaolusid, milleks on seose olemasolu Eesti riigiga või põhjendatud huvi kasutada Eesti riigi e-teenuseid[187]. Tõendama ja põhistama ei pea neid asjaolusid, mis on üldtuntud või haldusorganile teada, näiteks tegevust, mille kohta saab haldusorgan teavet riiklikest andmekogudest. E-residendi digitaalse isikutunnistuse taotluse saab isik esitada nii Politsei- ja Piirivalveametis kohapeal kui ka Eestisse saabumata Eesti välisesinduse konsulaarametnikule, kes edastab selle taotleja isikusamasuse kontrollimise ja biomeetriliste andmete võtmise järel omakorda läbivaatamiseks Politsei- ja Piirivalve-ametile[188]. Samas ei pea e-resident digitaalse isikutunnistuse taotluse esitamiseks isiklikult ilmuma dokumendi väljaandja asukohta või Eesti välisesindusse, kui ta ilmub menetluse käigus oma isiku tuvastamiseks või isikusamasuse kontrollimiseks isiklikult dokumendi väljaandja asukohta või taotluse või dokumendi väljastamisel Eesti välisesindusse. E-residendi digitaalse isikutunnistuse taotlemisel on haldusorgan kohustatud tuvastama taotleja isiku või kontrollima isiku isikusamasust. Selleks kohaldatakse e-residendi digitaalse isikutunnistuse taotleja suhtes välismaalaste seaduse § 24-28, 270, 271 ja § 272 lõikeid 1 ja 2, mis näevad ette alused ja menetluskorrad isikutuvastuseks isikut tõendava dokumendi alusel, biomeetriliste andmete, DNA-andmete või muude andmete põhjal. E-residentsuse taotleja on kohustatud võimaldama oma isiku tuvastamist ja isikusamasuse kontrollimist. Juhul, kui välismaalase või muu asjassepuutuva isiku isikut ei ole võimalik tuvastada või tema isikusamasust kontrollida, jäetakse e-residendi digitaalne isikutunnistus välja andmata.189 Käesoleval juhul on isikusamasuse kontrollil järgitud küll rakendusotsuse eelnõu *kõrge* taseme kvalifitseerimispunkti 1a. elemente, mis näevad ette dokumendi ja isikusamasuse kontrolli vastu autoriteetset allikat, ja punkti 2 kirjelduse, mille puhul on tegemist alternatiivse alusega juhuks, kui isikul puudub oma elukoha riigi isikut tõendav dokument, kuid

[187] ITDS § 20^6 lg 1.
[188] *Ibid*., § 20^7 lg 1^1.
[189] Õiguslikus mõttes on e-residendi digi-ID väljaandmise näol tegemist hüvega, mille saamiseks, sarnaselt viisaga, puudub isikul subjektiivne õigus. Rahvusvahelise õiguse põhimõtete kohaselt on riigil suveräänne õigus kontrollida välismaalaste riiki saabumist, riigis viibimist ja tagada vajaduse korral nende riigist lahkumine sunni kohaldamisega. E-residendi õiguslik seisund on oma olemuselt sarnane välismaalase õigusliku seisundiga – nii nagu välismaalasel ei ole subjektiivset õigust saada õigust Eestis viibimiseks, ei ole tal ka subjektiivset õigust saada Eesti isikut tõendav dokumenti. Kuna Eestis annab digitaalses keskkonnas kasutatav Eesti eID välismaalasele kohati suuremadki võimalused Eesti õigusruumis tegutsemiseks, on e-residendi digi-ID väljaandmisel kohaldatud samasid põhimõtteid, mida kohaldatakse välismaalastele viisa või elamisloa andmise otsustamisel.

problemaatiliseks osutub taas paralleelselt taseme *madal* täitmise punkti 3 sõnastus, mis kohustab isikusamasuse kontrolli käigus veenduma, et väidetav identiteet on autoriteetse allika andmetel olemas ning seejuures puuduvad teated tema surmast. Sellise kontrolli teostamine välisriigi kodanike suhtes, eriti kolmandatest riikidest pärit kodanike puhul, ei ole absoluutsena võimalik. Seega tuleks ka siin püüda läbirääkimiste käigus saada üle taseme *madal* punkti 3 sõnastuses surma fakti kontrollimise obligatoorsest nõudest ja teha sellest alternatiiv kontrollida kas isiku eksisteerimist *või* surma.

Muuhulgas on e-residendi digi-ID väljastamiseks ette nähtud ka erialus *kaaluka avaliku huvi korral* (ITDS § 20[11]), millise juhul puudub eelneva e-residendi digi-ID väljaandmise kirjelduse kohane isikutuvastamise ja isikusamasuse kontrolli menetlus. Nimelt võib kaaluka avaliku huvi korral Politsei- ja Piirivalveamet anda välja e-residendi digitaalse isikutunnistuse siseministri otsuse alusel, mis vormistatakse siseministri käskkirjaga. Sellisel juhul ei pea väljaandmisele eelnema isiku kirjalikku taotlust koos lisatavate andmete ja dokumentidega tingimusel, et Politsei- ja Piirivalveametile on teada andmed, mis tuleb dokumenti kanda. Antud määratluse kohaselt piisab isiku ees- ja perekonnanime, sünniaja, sünnikoha (riigi täpsusega) ja kodakondsuse teadmisest, kuivõrd ülejäänud digi-IDle kantavad andmed on sisult tehnilised[190]. Seega puudub e-residendi digi-ID väljastamiseks kaaluka avaliku huvi korral nõue isikutuvastamiseks. Muuhulgas on ette nähtud, et kaaluka avaliku huvi korral välja antud e-residendi digitaalse isikutunnistuse võib Politsei- ja Piirivalveamet väljastamiseks üle anda avalik-õiguslikke ülesandeid täitvale asutusele või isikule ning mitte vahetult digi-ID omanikule enesele, mis tähendab, et dokumendi väljastamisel ei nõuta ka muudele ITDS-s toodud eID-d kandvatele dokumentidele kohaldatavat isikusamasuse tuvastamise menetluse läbiviimist dokumendi väljaandmisel. Kontrolli ei teostata taotleva isiku isikut tõendava dokumendi kehtivuse osas, kuna kaaluka avaliku huvi korral väljastatava e-residendi digi-ID puhul puudub vajadus taotluse esitamiseks ega ka isikusamasuse kontrolli vastu autoriteetse allika kinnitust, nagu pole võimalik taotleja identifitseerimine sellena, kellena ta väidab end olevat, läbi tolle isiku ühe või mitme füüsilise karakteristiku võrdluse usaldusväärse allika poolt esitatud tõendi vastu, kuna isik ei pea esitama ei taotlust ega ühtki tõendit (*kõrge* taseme punkt 1a.). Alternatiivalusena väljapakutud kõrge taseme punktile 2 vastamiseks peaks isik, kes ei esita eID taotlemisel oma elukoha riigis väljaantud isikut tõendavat dokumenti, läbima liikmesriigis, kus eID väljaandmist taotletakse, isikutunnistuse

[190] Loetelu digi-IDle kantavatest andmetest leiab Vabariigi Valitsuse 26.08.2010 määruse nr 120 §-dest 4 ja 5.

taotlemiseks ettenähtud menetlusprotsessi, mis on kaaluka avaliku huvi korral väljaantava e-residendi eID menetluskorra kohaselt Eestis välistatud.

Eeltoodut arvesse võttes on Eesti e-residendi digi-ID väljaandmisprotseduuris mitmeid olulisi kõrvalekaldeid menetlusreeglitest, mida on komisjon ja liikmesriigid välja pakkunud eID-de usaldusväärsuse tasemete kvalifitseerimiseks. Läbiviidud eelanalüüsi kohaselt ei mahu e-residendi digi-ID väljapakutud e-identimise süsteemi usaldusväärsuse *kõrgemale* tasemele vastavate kriteeriumide raamidesse. Rakendusotsustuse eelnõu näeb hetkel väljapakutud sõnastuses ette ka *märkimisväärse* taseme määramise puhul isikuvastamise menetluse kohustuse[191], mille kohaselt peab minimaalselt ükskõik millise alternatiivi valikul olema tõendatud vähemalt, et isikul on olemas tema isikusamasust tõendavad riiklikult tunnustatud tõendid – mida kaaluka avaliku huvi korral väljaantavate e-residendi digi-IDde puhul Eestis läbi ei viida. Seega tuleks hinnata, kas antud e-identimise vahendi isikutuvastusprotseduur võiks kvalifitseeruda usaldusväärsuse tasemele *madal* vastavaks.

Madala taseme e-identimise süsteemi puhul olid eeldusteks isikutusamasuse tuvastamisel eeldus, et 1) isikul on olemas tema kohta väidetud isikusamasust tõendavad riiklikult tunnustatud tõendid – on mõistlik eeldada, et tunnustatud ärimehel, poliitikul või riigipeal (kellele võidakse potentsiaalselt avaliku huvi korral väljastada e-residendi digi-ID) on olemas tema isikut tõendav riiklik isikut tõendav dokument; 2) see tundub olevat kehtiv – kontrolle selleks, aga vastu autoriteetset allikat teostama ei pea; 3) autoriteetse allika andmetel on väidetav identiteet teadaolevalt olemas ega ole teada tema surmast ja 4) taotleja identifitseeritakse kasutades autoriteetsest allikast saadud teavet – antud taseme määratlemisel ei olnud isikule väljastatud isikut tõendavat dokumenti vastu autoriteetset allikat vajalik kontrollida, kuid nõutakse, et isiku eksistents oleks tõendatud ning puuduksid andmed selle ümberlükkamisest ning et isik oleks vastu autoriteetse allika andmeid identifitseeritud. "autoriteetse allika" definitsioon on niivõrd laia tõlgendusruumiga, et sinna alla loetakse ükskõik milline allikas (i.k. *any source*), mida võib pidada usaldusväärseks andmete, informatsiooni ja/või dokumentide edastamisel, mis isikut identifitseeriksid, siis võib püüda tõlgendada kaaluka avaliku huvi korral väljastatva e-residendi digi-ID puhul, et isik, kellele selline eID väljastatakse, on identifitseeritav ja tema elusolek (ning mitte surnud olemine) tuvastatud kas näiteks telefoni kõne või reaalaja meediapildi või postituse läbi, kuna madala taseme puhul ei esitata nõuet isikuga füüsiliselt kohtumiseks – vajalikud kontrollid võivad

[191] Vt Lisa 1, Rakendusotsuse eelnõu, lk 89-90.

olla teostatud kõik isikuga reaalselt kokku saamata. Seega võiks läbi "autoriteetse allika" definitsioonile jäetud laia tõlgendusruumi kvalifitseerida kaaluka avaliku huvi korral väljastatud Eesti e-residendi digi-ID rakendusotsuse eelnõu punkti 2.1.2 e-identimissüsteemi usaldusväärsuse tasemele *madal* vastavaks.

Käesolevast kerkib aga kaks küsimust:
1) kas ühe e-identimise vahendi erinevate väljaandmisprotseduuride kohane eID saab moodustada eIDAS määruse regulatsiooni kohaselt kaks e-identimise süsteemi ja
2) kui üks e-identimise vahend võib olla menetluskorrapõhiselt jaotatud kahte eri e-identimise süsteemi, mida tähendab see määruse artikkel 6 vastastikuse tunnustamise kohustuse kohaselt?

E-identimise süsteem on defineeritud eIDAS määruse artikli 3 punktis 4. Selles sätestatud määratluse kohaselt on e-identimise süsteem (*electronic identification scheme*) e-identimiseks vajalik süsteem, mille raames väljastatakse e-identimise vahendeid füüsilistele või juriidilistele isikutele või juriidilist isikut esindavatele füüsilistele isikutele. Seega tegemist on süsteemiga, mille raames väljastatakse e-identimise vahendeid ja need ei ole seotud rohkema kui ühtsetel alusel läbiviidava menetlusprotsessi läbi – ei ole vahet, kas neid antakse välja füüsilistele või juriidilistele isikutele või juriidilist isikut esindavatele füüsilistele isikutele või kas need on ühesugustel e-identimise vahenditel – määrab protsess, mille raames e-identimise vahendeid väljastatakse ning see loob e-identimise süsteemi. Seega võib esimesele küsimusele vastata, et eIDAS määrus võimaldab lugeda ühe e-identimise vahendi tulenevalt selle väljaandmise protseduurist ideeliselt jagatuks kahe erineva e-identimise süsteemi vahel. E-identimise süsteemi määratlemisele on võimalik läheneda kahel viisil: kas ühe e-identimise vahendi menetlusprotsessi põhiselt (juhul, kui kasutatakse erinevaid e-identimise vahendid ning nende väljaandmise protseduurid on erinevad) või e-identimise vahendite menetlusprotsessist tervikuna lähtudes (juhul, kui erinevate e-identimise vahendite menetlus viiakse läbi samade menetluspõhimõtete kohaselt). Kirjeldada tuleb süsteemi ehk menetlusprotsessi, mitte vahendit. Kuid milline mõju on sellel vastastikusele tunnustamisele artikkel 6 jõustumise valguses?

Artikkel 6 kohaselt peab liikmesriik, kui tema avalik sektor võimaldab internetipõhisele teenusele ligipääsu sealses riigis väljaantud eID-dega, võimaldama samale teenusele juurdepääsu ka teise liikmesriigi e-identimise vahendiga, mis on samale tasemele vastav või

sellest kõrgem. Madala taseme tunnustamine ei ole kohustus, kuna selle üle saab liikmesriik ise otsustada. Seega – hüpoteesi mõttes – kui Eesti kvalifitseerib ühe Eestis aktsepteeritud ja kasutatava e-identimise süsteemi eIDAS määruse usaldusväärsuse tasemele *madal* vastavaks, kuid kõik teised süsteemid vastavad tasemele *kõrge*, siis artikkel 6 vastava vastastikuse tunnustamise põhimõtte kohaselt tuleks võimaldada kõigi teiste liikmesriikide vähemalt tasemele *märkimisväärne* teavitatud e-identimise vahendite juurdepääs samadele süsteemidele, kuhu lastakse ligi meie oma e-identimise vastava süsteemi vahenditega. Ehk siis, kui Eesti võimaldab end e-residendi digi-IDga autentinud isikul teha õigusjõudu omavaid toiminguid nt Äriregistri ettevõtjaportaalis või Maksu- ja Tolliametis, siis tuleb võimaldada ka teiste liikmesriikide teavitatud e-identimise süsteemide *märkimisväärne* tasemega ligipääsu samadele süsteemidele. Tänased e-lahendused ei tee üldjuhul vahet, millise kvalifitseerituse tasemega e-ID'ga neisse logitakse, kui need ei ole just paroolikaardi- või salasõnapõhised, millistel juhtudel on teatud toimingud vastavate autentimislahenduste puhul välistatud (näiteks ei saa teha sularahatehinguid üle teatud piirmäära või digital-allkirjastada oma tahteavaldust). EIDga autentimise korral on aga süsteemipõhisete toimingupiirangute loomine märksa keerulisem.

Seega oleksime eelkirjeldatud olukorras sunnitud andma ligipääsu ka neile süsteemidele, mille puhul ei ole meie ID-kaardile võrdväärset isikutuvastust läbi viidud. See ei ole aga kahtlemata lahendus, mis oleks Eesti riigi ja kodanike huvides. Eeltoodud põhjustel tuleb kaaluda alternatiive.

Kuivõrd e-residendi digi-ID väljastamise protsess ei täida hetkel ära komisjoni poolt kavandatava rakendusotsuse kõrgema taseme usaldusväärsuse kriteeriume, tuleb analüüsida, kas mõistlikum oleks näiteks:

1) loobuda määruse artikkel 7 tingimustele vastavast ja artikkel 9 lg 1 kohasest e-residendi digi-ID süsteemi teavitamisest või
2) muuta ITDS regulatsiooni ning loobuda e-residendi digi-ID väljastamisest ilma isikutuvastus ning isikusamasuse kontrolli menetlusteta.

Esimese alternatiivi kasutamise korral mängivad rolli mitmed huvid. Kaalukausile asetatakse nii riskid teavitamata jäetud e-identimise süsteemi korral endiselt teisi süsteeme võrdväärselt vastastikku tunnustada kohustavast määruse artikkel 6-st, Eesti rahvusvahelisest mainest IT vallas kui ka e-residentsuse poliitilisest mandaadist. Arvestamist väärib kahtlemata ühelt poolt

Eesti riigi tõsiseltvõetavust elektroonilise identiteedi ja ühtse digitaalse siseturu valdkonna eestkõnelejana ja e-residentsuse protsessile püstitatud eesmärk tuua Eestisse uusi investeeringuid, töökohti, rahvusvahelist äritegevust ning sellega kaasnevat maksutulu[192], mida võib õõnestada avalikkuse potentsiaalne negatiivne tähelepanu, kui süsteemi võrdväärselt teiste Eestis kasutatavate e-identimise vahenditega ei kvalifitseerita ega teavitata, kuid tegelik probleem seisneb siiski selles, et vastavaid eID'sid võimaldatakse siseriiklikult kasutada võrdväärselt Eesti ID-kaardi eID-ga, seega tuleks hoolimata süsteemi teavitamata jätmisest võimaldada teise liikmesriigi võrdväärsetele nõuetele vastava teavitatud e-identimise süsteemidele ligipääs meil kasutatavatele avalikele e-teenustele, millega kaasnevad riskid on eeltoodus juba käsitlemist leidnud.

Tekib aga küsimus, **kuidas võib teine liikmesriik teada, millistele eeldustele vastab meie e-identimise vahend, millest ei ole Euroopa Komisjoni teavitatud?** Käesolevale küsimusele ei ole ühest vastust, mis toimiks alati iga liikmesriigi puhul, kuid Eesti kontekstis on kõikide riiklike identifitseerimisvahendite väljaandmine reguleeritud seadus(t)ega. Meie seadused on kättesaadavad ka inglise keeles, mistõttu võib igaüks huvi korral avada elektroonilise Riigi Teataja ja lugeda, milline on ettenähtud protseduur ühe või teise e-identimisvahendi taotlemiseks. Sellest lähtuvalt saab vastava võrdluse ja hindamise eIDAS määruse kvalifitseerimistasemete ja Eesti e-ID'de kontekstis läbi viia igaüks, kes on võimeline lugema ning aru saama selleks ettekirjutatud menetlusprotsessist. Vaidluse korral on vaidlustaval osapoolel võimalik pöörduda kaebusega Euroopa Komisjoni poole ning Euroopa Komisjon saab alustada kaebuse alusel rikkumismenetlust esitatud väidete ja tegeliku olukorra kontrollimiseks. Eeltoodust lähtuvalt, ei ole tegelikkuses ühegi süsteemi teavitamata jätmine lahendus vältimaks kohustust eIDAS määruse artikkel 6 jõustumisel tunnustada teise liikmesriigi eIDsid võrdväärselt omal kasutatavate eIDdega.

Antud olukorras oleks mõistlik läheneda võimalikule olukorrale läbimõeldult ning mitte jätta e-residendi digi-ID'st teavitamata, vaid luua süsteem – koostada rakendusplaan, mis ajakavastab ning järjestab Eesti riigi teavitatavad e-identimise süsteemid. E-residendi digi-ID võib olla teavitatavate hulgast viimane kui uusim kasutusel olev lahendus. Sel viisil jõuab tekkida nii liikmesriikide tasandil kui üleeuroopa piisavalt kokkupuuteid ja praktikat, et langetada sobiv otsus ka e-residentide e-identimise süsteemi registreerimise osas.

[192] Valitsusliidu tegevuskava, 08.04.2015. "E-riigi arendamine" p 4.15, lk 5. Arvutivõrgus: https://valitsus.ee/sites/default/files/content-editors/failid/re-sde-irl-valitsusliidu-lepe-2015.pdf (15.04.2015).

Teise alternatiivi valikul oleks positiivne mõju Eesti e-identimise süsteemidele tervikuna, kuivõrd selle läbi tekiks potentsiaalne võimalus kvalifitseerida Eestis kasutatavad e-identimise vahendid kõik usaldusväärsustasemele *kõrge* vastavaks, meil ei tuleks võimaldada vähem turvaliste süsteemide ligipääsu meie avaliku sektori elektroonsetele teenustele ning meil ei tarvitseks karta antud põhjusel kaotada ka oma riigi e-riigi maines. Küll aga vajaks antud olukorras rakendussätetega lahendamist küsimused, milline õiguslik staatus jääb ITDS § 20^{11} alusel juba väljaantud e-residentide digi-IDdele ja kas neid on võimalik edasi kasutada. Ehkki e-residendi digi-ID puhul on tegemist hüve mitte subjektiivse õigusega, on seadusmuudatuste kavandamisel ja läbiviimisel oluline ka õiguskindluse printsiibist[193] kinnipidamine.

Kõike eeltoodut kokku võttes on Eestil tugev potentsiaal kõigist meil kasutusel olevatest e-identimise süsteemidest teavitada eIDAS määrus artikkel 7 tingimustele vastavalt ning artikkel 9 lõike 1 kohaselt, kui rakendusotsuse läbirääkimistel leitakse käesolevas peatükis käsitletud elementide ümbersõnastamiseks piisavalt toetust ning loobutakse ITDS § 20^{11} alusel e-residentide eIDde väljastamisest.

2.3.3. Teavitatavate süsteemide koosvõime

Selleks, et vältida käesoleva töö esimeses peatükis kirjeldatud eIDAS-ele eelnenud perioodi riiklike identimissüsteemide killustatust, näeb eIDAS määrus liikmesriikidele ette artiklis 12 lg 5 kohustuse teha koostööd koosvõime artikli 9 lõike 1 kohaselt teavitatud e-identimise süsteemide ja nende e-identimise süsteemide vahel, millest liikmesriigid kavatsevad teavitada ning e-identimise süsteemide turvalisuse küsimustes. Selleks on eIDAS määruse alusel, arvestades eriti artikkel 12 lõiget 7, vastu võetud koosvõime raamistik[194], millega kehtestatakse menetluskord liikmesriikidevaheliseks koostööks e-identimise valdkonnas.

Liikmesriikide vaheline koostöö on ette nähtud hõlmama nii 1) teabe, kogemuste ja heade tavade vahetamist e-identimise süsteemide ning eelkõige koosvõime ja usaldusväärsuse tasemetega seotud tehniliste nõuete kohta, 2) teabe, kogemuste ja heade tavade vahetamist artiklis 8 sätestatud e-identimise süsteemide usaldusväärsuse tasemetega töötamise kohta,

[193] PS § 10.
[194] Komisjoni rakendusotsus (EL) 2015/296, ELT L 53, 24.02.2015, lk 14-20.

3) määruse kohaldamisalasse kuuluvate e-identimise süsteemide vastastikune hindamist ning 4) e-identimise sektoris toimuvate asjakohaste arengute analüüsimist[195].

Teabe, kogemuste ja heade tavade vahetamine liikmesriikide vahel muudab selgelt lihtsamaks e-identimise süsteemide väljatöötamise ning aitab kaasa nendevahelise tehnilise koosvõime saavutamisele. Vajadus selliseks koostööks on tingitud ühest küljest ajaloolisest süsteemide killustatusest, kuid teisalt käesoleva määruse kontektis iseäranis põhjendatud olukordades, kus tekib vajadus kohandada juba teavitatud e-identimise süsteeme või muuta süsteeme, mille kohta on teave liikmesriikidele esitatud enne teavitamist. Eriti on antud koostöövorm oluline võimalike intsidentide või oluliste arengute korral, mis mõjutavad e-identimise süsteemide koosvõimet ja turvalisust, kuna eIDAS määrusega on pööratud erilist tähelepanu turvalise e-identimise ja e-autentimise hõlbustamisele. Eesmärk on ennekõike turvaline digitaalne ühisturg ja seeläbi avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse elavdamine mitte vastupidi.

Komisjon on leidnud, et liikmesriikidevaheliseks koostööks on tarvis lihtsustatud menetlusi. E-identimise süsteemide koosvõimet ja turvalisust ei saa luua eri keeltes läbiviidatavate menetlustega. Selleks on ette nähtud koostöökeeleks inglise keel, kui liikmesriigid ise ei lepi kokku teisiti[196]. Inglise keele kasutamine koostöö käigus peaks hõlbustama koosvõime ja turvalisuse saavutamist erinevate e-identimise süsteemide vahel ning ei tohiks samas juba olemasolevate dokumentide tõlkimisel tekitada põhjendamatut koormust. Lisaks ühtsele keelele on oluline, et määratletud oleksid ka ühtsed kontaktpunktid, kelle vahel ning kaudu e-identimise süsteemide koosvõime ja turvaküsimustes asjakohast informatsiooni vahetada. E-identimise süsteemide eri elemente haldavad liikmesriikides erinevad asutused ja organid. Ka Eestis puudutavad antud küsimused nii Majandus- ja Kommunikatsiooniministeeriumi, Riigi Infosüsteemide Ameti, Siseministeeriumi, Välisministeeriumi, Politsei- ja Piirivalveameti, SA Sertifitseerimiskeskuse kui mitmete teiste asutuste ja organite tegevust. Ühtse kontaktpunkti määratlemine Eesti kontekstis on käsitlemist leidnud juba käesoleva töö peatükis 2.3.1.

Ühe koostööd hõlbustava ja e-identimise praktikaid ühtlustava meetmena on koosvõime raamistikus ette nähtud teavitatud e-identimise süsteemide **vastastikuse hindamise menetlus**. Vastastikuse hindamise protsessis osalemine ei ole liikmesriikidele obligatoorne, kuna kõik

[195] EIDAS määrus, artikkel 12 lg 6.
[196] Komisjoni rakendusotsus (EL) 2015/296, artikkel 2 lg 1.

sellega kaasnevad kulud tuleb kanda liikmesriikidel endil ja kõigi 28 liikmesriigi hindamises osalemine võib olla teatud juhtudel liikmesriikidele ülejõu käiv. Vastastikkust hindamist käsitletakse pigem kui õppeprotsessi, mis aitab liikmesriikide vahel luua usaldust ning loob teavitatud e-identimise süsteemide vahel tugevamat koosvõimet ja turvalisust.

Hindamisprotsessi algatamiseks on aga kaks võimalikku moodust – esiteks, kas liikmesriik ise taotleb oma e-identimise süsteemi vastastikust hindamist või teiseks, kui liikmesriik või liikmesriigid avaldavad soovi teise liikmesriigi e-identimise süsteemi vastastikuse hindamise läbiviimiseks. Sellises taotluses teise liikmesriigi e-identimise süsteemi hinnata tuleb põhjendada vastastikuse hindamise läbiviimise soovi ja selgitada, kuidas taoline hindamine edendaks liikmesriikide e-identimise süsteemide koosvõimet või turvalisust. Seega ehkki vastastikusest hindamisest osa võtmine on liikmesriikidele vabatahtlik, ei ole seda viimases variandis kirjeldatud valik saada hinnatud, kui sellist soovi avaldab üks või mitu liikmesriiki. Liikmesriik, kelle e-identimise süsteemi suhtes viiakse läbi vastastikune hindamine, ei saa keelduda ühegi vastastikust hindamist teostava liikmesriigi osalemisest hindamise protsessis[197]. Saab küll huvide konflikti korral keelata mis tahes esindaja osaluse vastastikuse hindamise protsessis, kuid hindamisest enesest keelduda alust ei ole. Tuleb möönda, et komisjoni poolt ettenähtud hindamismenetlus ei näe ette meetmeid juhuks, kui liikmesriik otsustab eirata saada hinnatud ja näiteks ei esita dokumente või andmeid, mida hindamiseks küsitud on – antud vastastikuses hindamismenetluses puuduvad n.ö sanktsioonid, kui koosvõime raamistikku mitte täita. Sellisel juhul on komisjonil Euroopa Liidu aluslepingust tulenevalt õigus algatada rikkumismenetlus[198].

Kuivõrd aga määruse artikkel 7 punkti g kohaselt, mis viitab artikkel 12 lõikest 5 tulenevale kohustusele, teevad liikmesriigid koostööd artikli 9 lõike 1 kohaselt teavitatud e-identimise süsteemide ja nende e-identimise süsteemide vahel, millest liikmesriigid kavatsevad teavitada, ning e-identimise süsteemide turvalisuse küsimustes, siis sellest tulenevalt on antud koosvõime raamistiku kohasesse hindamismenetlusse sisenemine võimalik teataval määral ette valida – kui otsustatakse teavitada, tuleb arvestada kaasnevate koosvõime raamistikust tulenevate kohustustega.

[197] Koosvõime raamistiku artikkel 7 lg 2.

[198] Euroopa Liidu toimimise lepingu konsolideeritud versioon. Artikkel 258: "Kui komisjon on arvamusel, et liikmesriik ei ole täitnud aluslepingutest tulenevat kohustust, esitab ta selle kohta oma põhjendatud arvamuse, olles andnud asjassepuutuvale riigile võimaluse esitada oma seisukoht. Kui asjassepuutuv riik ei järgi esitatud arvamust komisjoni seatud tähtaja jooksul, võib komisjon anda asja Euroopa Liidu Kohtusse."

EIDAS määruse artikli 12 lõigetes 5 ja 6 sätestatud eesmärkide saavutamiseks vajaliku menetluskorra hõlbustamiseks luuakse muuhulgas ka **koostöövõrk**, mille eesmärk on tagada foorumi loomine ja töölerakendamine, mis hõlmaks kõiki liikmesriike ning kaasaks neid ametlikult tegema koostööd koosvõime raamistiku ülalpidamise praktiliste aspektide vallas. Koostöövõrgul on pädevus avaldada arvamusi, millest kõik teavitamise osalised peaksid koostöö-, teavitamis- ja koosvõimemenetlustes lähtuma, ning anda vastastikuse hindamise protsessi tõhususe tagamiseks suuniseid, kuid neil arvamustel ja suunistel ei ole taaskord kohustavat õigusjõudu. Koostöövõrgu liikmeteks saavad olla kõik liikmesriigid ning Euroopa Majanduspiirkonna riigid[199] ning koostöövõrgu koosolekuid juhatab komisjon[200].

Koostöövõrgule on antud volitused:

1) hõlbustada eIDAS määruse artikli 12 lõigetes 5-6 ettenähtud liikmesriikidevahelist koostööd koosvõime raamistiku loomise ja toimimise vallas teabevahetuse kaudu,
2) luua kõigi e-identimise küsimustega seoses tõhusa teabevahetuse meetodid,
3) analüüsida e-identimise sektori asjakohaseid arenguid ning arutada e-identimise süsteemide koosvõime ja turvalisusega seonduvate heade tavade üle ja töötada vastavad tavad välja,
4) võtta vastu arvamusi eIDAS määruse artikli 12 lõigetes 2-4 osutatud koosvõime raamistiku arengute kohta,
5) võtta vastu arvamusi minimaalsete tehniliste kirjelduste, standardite ja menetluste arengute kohta seoses usaldusväärsuse tasemetega, mis on sätestatud eIDAS määruse artikli 8 lõike 3 kohaselt vastu võetud rakendusaktis ning kõnealusele rakendusaktile lisatud suunistes,
6) võtta vastu suuniseid vastastikuse hindamise ulatuse ja korra kohta,
7) analüüsida vastastikuse hindamise tulemusi vastavalt koosvõime raamistiku artiklile 11,
8) kontrollida täidetud teatisevormi kavandeid,
9) võtta vastu arvamusi selle kohta, kuidas teavitatav e-identimise süsteem, mille kirjeldus esitati vastavalt eIDAS määruse artikli 7 punktile g, vastab kõnealuse määruse artiklis 7, artikli 8 lõigetes 1-2 ja artikli 12 lõikes 1 ning kõnealuse määruse artikli 8 lõikes 3 osutatud rakendusaktis sätestatud nõuetele.

[199] Koosvõime raamistiku artikkel 15 lg 1.
[200] *Ibid*., art 16 lg 1.

Liikmesriigid peavad oma soovist saada hinnatud või soovist teist liikmesriiki hinnata andma teada koostöövõrgule. Samuti tuleb igal vastastikuses hindamises osaleda otsustaval liikmesriigil teavitada sellest koostöövõrku. Seega on koostöövõrgul oluline korraldav ja koordineeriv ning analüüsiv ja suunav roll, aga ka kriitiline tähtsus ühtse praktika ja toimiva võrgustiku juurutamisel.

Liikmesriik, kelle suhtes viiakse läbi e-identimise süsteemi vastastikust hindamist peab koostöövõrgule esitama järgmise teabe:

1) e-identimise süsteem, mille suhtes vastastikune hindamine läbi viiakse,
2) vastastikust hindamist teostav(ad) liikmesriik või liikmesriigid,
3) oodatava tulemuse koostöövõrgule esitamise tähtaeg ning
4) vastastikuse hindamise läbiviimise menetluskord vastavalt koosvõime raamistiku artikli 9 lõikele 2.[201]

Vastastikune hindamine ise võib hõlmata nii asjaomaste dokumentide hindamist, menetluste kontrolli, tehnilisi seminare kui sõltumatu kolmanda isiku hinnangu arvestamist[202]. Kirjeldatud protsessi viiakse läbi liikmesriikide poolt ühiselt, kuid liikmesriigid valivad endi seast ühe esindaja, kes vastastikuse hindamise läbiviimise protsessi koordineeriks[203]. Vastastikuse hindamise läbiviivatel liikmesriikidel lasub ühtlasi ülesanne ühe kuu jooksul peale vastastikuse hindamise läbiviimist valmistada ette aruanne ning esitada see koostöövõrgule[204], mida koostöövõrk seejärel analüüsib ja võtab vastu arvamuse, kuidas teavitatav e-identimise süsteem eIDAS määrusest tulenevatele nõuetele[205] vastab. Peale niisuguse hindamise läbimist ei pea liikmesriigi sama e-identimise süsteem läbima enam uut e-identimise süsteemi vastastikust hindamist kuni järgneva kahe aasta jooksul. See klausel ei kehti aga juhul, kui koostöövõrgus lepitakse kokku teisiti[206].

Seega käesoleva vastastikuse hindamise läbi saavad teavitatavad e-identimise süsteemid enda kvalifikatsioonitaseme verifitseerida eIDAS määruse artikkel 12 lõikes 1 sätestatule ning artikkel 8 lõike 3 alusel vastuvõetavale rakendusaktile vastavalt.

[201] Koosvõime raamistiku artikkel 8 lõige 3.
[202] *Ibid*., art 10 lõige 3.
[203] *Ibid*., art 10 lõige 1.
[204] *Ibid*., art 11.
[205] Vastavst kontrollitakse määruse artiklites 7, 8 lõigetes 1-2 ja 12 lõikes 1 ning artikli 8 lõikes 3 osutatud rakendusaktis sätestatud nõuetele.
[206] Koosvõime raamistiku artikkel 8 lõige 4.

KOKKUVÕTE

Euroopa Liidu digitaalse siseturu kõige olulisemad probleemid piiriülesel e-teenuste osutamisel on nii ajalooliselt kui käesolevalt seotud valdavas osas elektroonse identiteediga. Riigisiseselt on enamikes liikmesriikides autentimise ja digiallkirjastamise küsimused lahendatud, kuid selleks, et erinevad tehnilised ja protseduurilised lahendused toimiksid üle riigipiiride, on puudunud selge ühtne süsteem nende üleeuroopaliseks koosvõimeks. Autor on selgitanud seetõttu e-identimise ühtlustamise vajalikkust Euroopa Liidu majandusruumis ning käsitlenud eraldi Eesti osa nimetatud protsessis. Alates 23. juulil 2014 eIDAS määruse vastuvõtmisest on kontseptuaalne olukord pöördeliselt muutunud. EIDAS määrusega tagatakse[207] ühtselt nii füüsilistele isikutele kui ettevõtetele võimalus kasutada riiklike elektrooniliste IDde pakutavat juurdepääsu avalikele teenustele ka teistes liikmesriikides.

EIDAS määrus on otsekohalduv ning selle reguleerimisala ei saa Eesti oma seadustega (ümber)reguleerida. Eestis ollakse seevastu enne eIDAS määruse vastuvõtmist kasutatud juba laialdaselt ning peagi 15 aastat oma riiklikku eID-d ning selle aja jooksul on riiklike e-identimise vahendite ring pidevalt kasvanud. Autor on andnud käesolevas magistritöös ülevaate e-identiteedi ajaloolisest kujunemisest nii Eestis kui selle paralleelarengust Euroopa Liidus ning käsitlenud lähemalt Eestis kasutusel olevatid e-identimise vahendeid.

EIDAS näeb liikmesriikidele ette kohustuse tunnustada teiste liikmesriikide teavitatud e-identimise vahendeid. E-identimise vahendid klassifitseeritakse e-identimise süsteemidesse ja liikmesriikidel on seejuures vaba voli otsustada, kas oma e-identimise süsteemidest määruse alusel komisjoni teavitada või mitte, kuid hoolimata tehtavast valikust, tuleb kõigil liikmesriikidel tunnustada samaväärsele või kõrgemale tasemele vastava teise liikmesriigi eID-d ning võimaldada sellega riiklikele e-teenustele siseriikliku eIDga võrreldes samaväärne ligipääs. Seega eeldab eIDAS määrus uute mängureeglite täitmiseks riiklike e-identimise vahendite süstematiseerimist ning neile vastavate tasemete määramist.

Autor on käesolevas magistritöös põhjalikult analüüsinud ning hinnanud, millised on tagajärjed Eesti riigile eIDAS määruse kohaselt e-identimise süsteemidest komisjoni teavitamisel ja teavitamata jätmisel, millistele eIDAS määruse kehtestatavatele usaldusväärsuse tasemetele Eesti riigi e-identimise süsteemid kvalifitseeruvad, millised on

[207] Selle e-identiteedi osa sätete jõustumisel 2018.

selleks läbitava protsessi keerukused ja väljakutsed ning kuidas neid ületada, esitanud analüüsist lähtuvalt ettepanekud e-identimise süsteemide määratlemiseks, käimasoleva eIDAS määruse alusel vastuvõetava rakendusakti eelnõu mõjutamiseks ning siseriiklikult eIDde väljaandmisprotsessi ümberreguleerimiseks e-residendi digi-ID väljaandmisel kaaluka avaliku huvi korral. Autori peaülesandeks käesolevas magistritöö teises osas oli jõuda läbi analüüsi selguseni, kuidas e-identimise küsimustes eIDAS määrust Eestis kohaldada. Samuti on autor analüüsinud uusi menetlusprotsesse, mis vastavate sätete jõustumisest alates liikmesriikidele kohalduvad ning varasemat ajaloos ilmnenud identimisvahentite koostoime puudusest tingitud killustatust edaspidi vältida võimaldavad.

Selleks, et Eesti elanike huvides eIDAS määruse e-identimise regulatsiooni parimal viisil rakendada tuleb autori hinnangul Eesti e-identimise vahenditest Euroopa Komisjoni vastavalt eIDAS määruse artiklite 7 ja 9 lõike 1 nõuetele teavitada. Teavitamata jätmisega kaasnevad arvestatavad riskid: 1) võimaldada teise liikmesriigi võrdväärsetele nõuetele vastava teavitatud e-identimise süsteemidele ligipääs meil kasutatavatele avalikele e-teenustele, mille usaldusväärsuse taset ei peeta teiste liikmesriikide poolt *kõrgeks* eIDAS määruse mõttes; 2) piiratakse eIDAS määruse poolt võimaldatud üleeuroopaline ligipääs Eesti eID kasutajatele teiste liikmesriikide riiklikele e-teenustele kuivõrd ligipääs on automaatne vaid teavitatud e-identimise vahenditele ning 3) teise liikmesriigi eID Eestis kasutatavaga võrdväärseks mittepidamisel ja vaidluse korral sellele ligipääsu mittevõimaldamisel Euroopa Komisjoni poolt algatatava rikkumismenetluse läbiviimiseks ja võimalikuks trahvimiseks.

Eesti e-identimise vahendid tuleb paigutada süsteemi, mis seob nad väljaantava menetlusprotsessi kaudu. Üks e-identimise vahend ei pea moodustama üht e-idenitmise süsteemi, vaid e-identimise süsteemi moodustab protsess – menetluskord – mille alusel ning läbi mille liikmesriik e-identimise vahendeid väljastab. Eestis kasutusel olevad e-identimise vahendid on seotavad ühte süsteemi, erisusega e-residendi digi-ID osas, kuivõrd selle puhul ITDS-is § 20^{11} ettenähtud erialus e-residendi digi-ID väljastamiseks kaaluka avaliku huvi korral, ei täida ära isikusamasuse tuvastamise ja kontrolli menetlusnõudeid, mistõttu ei mahu see teiste e-identimise vahenditega sama süsteemi raamidesse. E-residendi digi-ID väljajätmine antud süsteemist ei kõrvalda aga vastastikuse tunnustamise nõudest tõusetuvat probleemi, mille kohaselt tuleb liikmesriigil ligi lasta kõigi teiste liikmesriikide võrdväärsele tasemele vastavat (või sellest kõrgemat) e-identimise vahendit, millele kvalifitseerub tema siseriiklik e-identimise vahend (v.a kui see on *madal*, millisel juhul tuleb aktsepteerida teisi

vähemalt *märkimisväärsele* tasemele vastavaid liikmesriikide eIDsid). Kuivõrd antud juhul viiks ITDS § 20[11] alusel väljaantav e-residendi digi-ID e-identimise süsteemi usaldusväärsuse tasemele *madal* vastavaks, tuleks Eestil võimaldada eIDAS määruse artikli 6 lg 1 punktidest (b) ja (c) tulenevalt ligipääs ka kõigile teistele liikmesriikide eID-dele, mis täidavad ära kvalifikatsioonitaseme *märkimisväärne*, ja võimaldada neile võrdsetel alusel ligipääs Eesti riiklikele e-teenustele, millele pääsevad ligi e-residendi digi-ID kasutajad (nt e-maksuamet, Äriregistri ettevõtjaportaal, e-tervis jm). Niisuguse lähenemisega loodaks arvestatav turvarisk Eesti riiklike e-teenustele. Antud olukorra ületamiseks teeb autor ettepaneku muuta ITDS-i ning loobuda alusest kaaluka avaliku huvi korral isikutele e-IDde väljastamiseks.

EIDAS määrus näeb e-identimise vallas ette liikmesriikidele kohustuse teha koostööd teiste liikmesriikidega sõltumata e-identimise süsteemi(de)st teavitamisest. Sellele vaatamata on käesoleva töö autori hinnangul koostöö Eesti eIDde kasutajate vaates viljakam, kui Eesti e-identimise vahenditest vastavalt eIDAS määrusele Euroopa Komisjoni teavitab. See võimaldab saada meie eID kasutajatel täismahus kasu ka eIDAS koosvõime raamistiku alusel loodava koostöövõrgu tulemustest. Laiapõhjaline aga samas süstematiseeritud ja reglementeeritud koostöö tagab tegelikkuses riiklike e-identimise süsteemide üleeuroopalise suurema harmoniseerituse, (ennekõike) Euroopa Liidu kodanikele võimaluse saada reaalset ja suuremat kasu ühtse digitaalse siseturu toimimisest, luua võimalusi erasektorile käesoleva regulatsiooniga kaasatulemiseks ning seeläbi elavdada nii Eesti kui Euroopa Liidu majandust tervikuna.

Käesoleva töö autor on seisukohal, et antud eIDAS regulatsioonile tuleb pöörata suuremat ühiskonna tähelepanu ja seista aktiivselt nii Eesti kui Euroopa Liidu ühiste huvide eest, seda nii erasektori informeerimises, kaasatõmbamises, kui käesoleval hetkel veel määruse alusel vastuvõetavate rakenduaktide läbirääkimistes. Õigusloomeline protsess ei ole veel lõppenud ja selle tulemustest sõltub suuresti algava eIDAS ajastu Eesti digitaalne käekäik, kas me püsime teenäitajad ning muudame oma elanikele digitaalse asjajamise riigipiiride-üleselt Euroopa Liidus lihtsamaks või jätame endid ilma hüvedest, mida eIDAS regulatsioon endas pakub.

SUMMARY

E-identity in the legal system of Estonia and European Union: applying Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market in Estonia – a study of its development, problems tackled and challenges ahead

The most important problem of the European Union digital internal market at the present time in the field of cross-border online services is largely related to electronic identity. The majority of Member States have authentication and digital signature issues solved out at their national level, but so that the various technical and procedural solutions would operate also across borders, a clear unified system has been missing for the European interoperability among them. In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognized in other Member States. The author of this thesis has therefore explained the necessity of harmonizing e-identification systems in the European Union's internal market, while paying separate attention to the role of Estonia in that process. Since 23 July 2014, the adoption of the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (also known as eIDAS Regulation), the situation has conceptually dramatically changed. After the electronic identification chapter of the eIDAS (*electronic IDentification and Authentication Services*) Regulation will enter into force in 2018, every individual and business who uses national electronic ID scheme has the potential to use it's national eID for accessing to public services offered in other Member States. These changes will mark the beginning of a new era in the digital internal market of EU.

EIDAS Regulation is directly applicable in all Member States and its scope cannot be adjusted with one's own legislation and laws. In contrast, even before the adoption of eIDAS Regulation, Estonia had used its own national electronic identification means approximately 15 years for personal and corporate use. The range of eID-means has continued to increase during that time from the very first identity card in the beginning of 2001. This identity card already allowed electronic identification and digital signing. Furthermore, the later eID-means as a digital identity card, a residence permit card, a mobile-ID and finally the latest

e-resident's digital identity card are all being used for the purpose of electronic identification. The author has given herein an overview of the legal aspects and procedural development of the e-identification and its tools, both in Estonia and in the European Union. The author has also made a more in depth analysis regarding the legal aspects of e-identification system and its means in Estonia.

The author has also analyzed and explained the main purpose of the e-identification regulation in the eIDAS Regulation. EIDAS stipulates the obligation for Member States to recognize other Member States' notified e-identification means. National electronic identification means are systematized in e-identification schemes and the e-identification schemes are determined to a certain assurance level laid down in Article 8 of the eIDAS Regulation. Member States have the freedom to choose whether or not to notify the European Commission of their e-identification schemes under the eIDAS Regulation. However, in spite of their decision, all Member States are obliged to recognize an equivalent or higher assurance level eIDs of another Member States for their own public sector online services. Under the eIDAS Regulation, the electronic identification means that are issued in one Member State shall be recognized in another Member State for the purpose of cross-border authentication when electronic identification means and authentication are required by the national law or by administrative practice to access services provided by a public sector body in the first Member State.

The author has made a thorough analysis and assessment of the consequences for Estonia when it chooses between notifying its e-identification schemes according to the Regulation or when it chooses not to. The author has analyzed what type of assurance level the Estonian national e-identification scheme(s) would meet according to the eIDAS Regulation and the final draft of an implementing act that will be adopted under the eIDAS Regulation Art 8 and 9(1) – what type of complexities and challenges Estonia meets during this task and how to overcome them. The author has also proposed changes for the wording in the beforementioned implementing act's draft, plus necessary changes for the national regulation to fully comply with the eIDAS Regulation.

In the second part of this thesis, the author has reached a conclusion how to apply the eIDAS Regulation in Estonia so that the Estonian citizens could enjoy the full benefits of the digital internal market through the eIDAS Regulation. The author has also analyzed the new

procedural rules that apply to Member States when the relevant provisions of e-identification will enter into force.

Through a comprehensive analysis the author has reached to an understanding that it is in the best interest for its residents when Estonia chooses to notify of its eID schemes to the Commission under the Articles 7 and 9(1) of eIDAS. Otherwise Estonia will face the following risks:

1) Estonia could be obliged to recognize other Member States' eIDs which level of reliability might not have the same high level or reliability as the Estonian national eID's;
2) Estonian residents' use of their eIDs will be limited in other Member States when Estonia will not notify its eID schemes, since Member States are obliged to mutually recognize only these eID schemes which are being notified according the eIDAS Regulation; and
3) a possible infringement procedure by the European Commission and fine in case of a dispute between Member States, where Estonia might not give access to its public sector online services to another Member State's eID, because the other Member State's eID might not be considered equivalent to Estonian national eID's, which has not been notified (therefore not assessed according to the assurance levels in Art 8 of eIDAS Regulation).

Estonian national e-identification means should be placed in a scheme which links the eID means through the procedural rules of their issuance. One eID scheme does not necessarily mean one electronic identification means, since one scheme can describe several eID means when their procedural rules and technical specifications comply with the appropriate assurance level laid down in eIDAS Regulation and the implementing act adopted according to Articles 8 and 9(1) of the eIDAS Regulation.

Estonia's e-identification means could be classified in one eID scheme, albeit one exception: the e-resident's digital identity card. The e-resident's digital identity card (when it's issued under the paragraph 20^{11} of the Estonian national Identity Documents Act) does not meet the criteria that are foreseen for the higher assurance level eIDs[208], that other means used for

[208] The e-resident's digital identity card can be issued under the provision of Estonian national Identity Documents Act § 20^{11} allowing to issue the e-resident's digital identity card in case of *substantial public interest*

electronic identification could fulfill (such as an identity card, a digital identity card, a residence permit card and mobile-ID). Excluding the e-resident's digital identity card from the notified eID scheme would not solve the issue from the mutual recognition obligation. After a thorough analysis it appeared that the Estonian e-resident's digital identity card might be equivalent to the assurance level *low* rather than level *substantial* or *high* (which both require certain procedures of person's identification to be carried out). This means that Estonia would be obliged to recognize other Member States' eIDs up from the level of *substantial*, as stipulated in Article 6 (1) under a and c of the eIDAS Regulation[209]. E-identification card holders of other Member States would be thereof allowed to access Estonian public online services, which are accessible with the Estonian e-resident's digital identity card, such as the e-Tax Board, Company Registration Portal or e-Health services etc. Such an approach would create a significant security risk for the public online services for Estonia. For overcoming that difficult situation the author has made a proposal to amend the national Identity Documents Act (IDA) and invalidate the provision that gives the right to issue national eID to non-residents in case of a substantial public interest (IDA § 20[11]).

The eIDAS Regulation also foresees the possibility for Member States to cooperate with other Member States in the field of e-identification, regardless the fact whether their e-identification scheme(s) are being notified to the European Commission or not. In the author's opinion the cooperation for Estonia's eID users would be more fruitful when Estonia would notify the European Commission of its eID scheme. Namely, this would allow Estonian eID users to get the full benefit of the interoperability framework put into place by eIDAS.

Broad but again systematized and regulated cooperation will ensure in practice a higher harmonization of national e-identification schemes around the European Union. Moreover, for the citizens of the European Union to truly benefit from the digital single market mutual recognition of electronic identification schemes are necessary. Through creating opportunities for the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions, it will stimulate the economy both in Estonia and in the European Union.

In this study the author is of the opinion that more attention needs to be paid to the eIDAS

---

without any identifying evidence required or identity checks made against authoritative sources.

[209] eIDs corresponding to the assurance level *low* are excluded from the obligation of mutual recognition.

Regulation both on the national and European level. Estonia needs to stand actively for the common interests of Estonia and the European Union. Especially until the legislative process under eIDAS Regulation has come to an end, so that the outcome would be truly beneficial for the economy in EU as a total. It is of equally importance that Estonia as a Member State would not exclude itself from the benefits that the eIDAS Regulation offers for notified countries.

KASUTATUD LÜHENDID

DAS – digitalallkirja seadus

EGDI – ÜRO e-valitsuste uuringus kasutatud e-riigi arenguindeks (i.k *e-Government Development Index*)

eID – elektroonilise identiteet, mis on kantud elektroonilise identimise vahendile

eIDAS – Euroopa Parlamendi ja nõukogu (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 (i.k *electronic IDentification and Authentication Services regulation*)

EL – Euroopa Liit

EKo – Euroopa Liidu Kohtu otsus

IKT – informatsiooni- ja kommunikatsiooni tehnoloogia

ITDS – isikut tõendavate dokumentide seadus

KOM – Euroopa Komisjon

PSTS – EV põhiseaduse täiendamise seadus

RIA – Riigi Infosüsteemide Amet

SK – Sertifitseerimiskeskus

STORK – Euroopa Komisjoni suurprojekt (i.k *Secure identity acrOss boRders linked*), mille eesmärgiks oli luau ühtne Euroopa eID platvorm, mis võimaldaks mistahes EL liikmesriigi e-riigi teenustele ligipääsu kõigile EL kodanikele nende oma riigi eIDga

ÜRO – Ühinenud Rahvaste Organisatsioon

KASUTATUD MATERJALIDE LOETELU

Kasutatud kirjandus

1. Annus, Ruth. E-residentsus. Juridica, 2014, nr 10, lk 740-750.
2. Arora, Siddharta. National e-ID card schemes: A European overview. Information Security Technical Report. May 2008. Volume 13, Issue 2, p. 46-53.
3. E-Government for the Future We Want. United Nations E-Government Survey 2014. United Nations. New York, 2014, p. 1-284.
   Arvutivõrgus: http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf, 24.04.2015.
4. Everett, Catherine. E-Identity: an isuse of trust. Computer Fraud and Security. Elsevier B.V. March 2011, p. 8-10.
5. Everett, Catherine. Will the e-identity STORK deliver a European baby? Computer Fraud and Security. Elsevier B.V. August 2009, p. 13-16.
6. Feasibility Study on an Electronic Identification, Authentication and Signature Policy (IAS). European Union 2013, p. 13-422.
7. Henry Lauren. Information Privacy and Data Security. April 29, 2015. Cardozo Law Review de Novo, 2015, Forthcoming, p. 107-118. Available at SSRN: http://ssrn.com/abstract=2600495, 01.05.2015.
8. Jakisch, Gerhard. E-signature versus E-Identity: the creation of the digital citizen. Database and Expert Systems Applications. IEEE Xplore Digital Abstract, 2000, p. 312-316.
9. Kalvet, T., Tiits, M., Hinsberg, H. E-teenuste kasutamise tulemuslikkus ja mõju. Uuringu aruanne. Balti Uuringute Instituut ja Poliitikauuringute Keskus Praxis. Tallinn, 2013. Lk 12-190. Arvutivõrgus: http://www.praxis.ee/fileadmin/tarmo/Projektid/Valitsemine_ja_kodanike%C3%BChiskond/E-teenuste_kasutamise_tulemuslikkus_ja_moju.pdf, 10.04.2015.
10. Laurent, M., Denouël, J., Levallois-Barth, C., Waelbroeck, P. Digital Identity Management, 1st Edition, Elsevier Ltd. 2015, p. 1-45.
11. Mahler, Tobias. Governance Models for Interoperable Electronic Identities. Journal of International Commercial Law and Technology, 2013. Vol. 8, No. 2, p. 148-159.
12. Myhr, Thomas. Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution or I am 621216-1318, but I am also 161262-43774. Do

you know who I am?. Information Security Technical Report. May 2008. Volume 13, Issue 2, p. 76-82.

13. Price, Geraint. The benefiits and drawbacks of using electronic identities. Information Security Technical Report. May 2008. Volume 13, Issue 2, p. 95-103.
14. Reed, Chris. Taking sides on technology neutrality. *SCRIPTed* – A Journal of Law, Technology & Society. Volume 4, Issue 3, p. 263-284.
15. Strategy to Combat Transnational Organized Crime. US 2011, p. 3-28. Online: https://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf, 01.05.2015.
16. Study for Public Services Online. Assessing User Centric eGovernment performance in Europe – eGovernment Benchmark 2012. European Union, 2013, p. 11-74. Online: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/eGov%20Benchmark%202012%20insight%20report%20published%20version%200.1%20_0.pdf, 03.04.2015.
17. Sullivan, C., Stalla-Bourdillon, S. Digital identity and French personality rights – A Way forward in recognising and protecting an individual's rights in his/her digital identity. Computer Law and Security Review, 2015, p. 268-279.
18. Truuväli, E.-J., *et al* (toim). Eesti Vabariigi Põhiseadus. Kommenteeritud vlj. Veebiväljaanne. Tartu Ülikool 2012. Arvutivõrgus: http://www.pohiseadus.ee/, 24.04.2015.
19. Whitley, Edgar A. On technology neutral policies for e-identity: A critical reflection based on UK identity policy. Journal of International Commercial Law and Technology, 2013. Vol. 8, No. 2, p. 134-147.
20. Williams, John F. Trace Evidence. Journal of Criminal Law, Criminology and Police Science. Northwestern University School of Law, 1958. Volume 49, Issue 3, p. 285-288.
21. Williams, M. L. Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. British Journal of Criminology. Published online: http://bjc.oxfordjournals.org/content/early/2015/04/27/bjc.azv011.full.pdf+html?sid=5601ffe5-8aec-45c8-b12f-06c32f1fca5f, April 27, 2015, p. 1-28.
22. Wu, Xiang-dong; Zhou, Jian. E-commerce „identity" – – a digital certificate. Journal of Chemical and Pharmaceutical Research, 2014. Volume 6, Issue 10, p. 652-654.
23. Xin-sheng, Lei. E-commerce safety technology. 1st edition. National Defence Industry Press. Beijing, 2012, p. 35-40.

Kasutatud normatiivmaterjalid

Rahvusvahelised normatiivmaterjalid

24. Convention relating to the Status of Refugees, Geneva, 28 July 1951. 22 April 1954, No. 2545. United Nations, Treaty Series, vol. 189, p 137-158.
25. Euroopa Liidu leping (konsolideeritud versioon). – ELT C 326, 26.10.2012. Lk 13-46.
26. Euroopa Liidu toimimise lepingu konsolideeritud versioon. – ELT C 326, 26.10.2012. Lk 47-201.
27. Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 23.11.1995. Lk 31-50.
28. Euroopa Parlamendi ja nõukogu 13. detsembri 1999. aasta direktiiv 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta. – EÜT L 13, 19.1.2000. Lk 12-20.
29. Euroopa Parlamendi ja nõukogu direktiiv 2002/21/EÜ, 7. märts 2002, elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv). – EÜT L 108, 24.4.2002. Lk 33–50.
30. Euroopa Parlamendi ja nõukogu direktiiv 2006/123/EÜ teenuste kohta siseturul. – ELT L 376, 27.12.2006. Lk 36-68.
31. Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 765/2008, 9. juuli 2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (EMPs kohaldatav tekst). ELT L 218, 13.8.2008. Lk 30-47.
32. 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, 28.8.2014. Lk 73–114.
33. Komisjoni rakendusotsus (EL) 2015/296, 24. veebruar 2015, millega kehtestatakse menetluskord liikmesriikidevaheliseks koostööks e-identimise valdkonnas vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 7 (EMPs kohaldatav tekst). – ELT L 53, 25.2.2015. Lk 14-20.
34. Pagulasseisundi konventsioon. 27. juuli 1951. – RT II 1997, 6, 26.

Riigisisesed normatiivmaterjalid

35. Asjaõigusseadus. 09. juuni 1993. – RT I 1993, 39, 590; RT I, 29.06.2014, 109.

36. Digitaalallkirja seadus. 8. märts 2000. – RT I 2000, 26, 150; RT I, 29.06.2014, 109.
37. Digitaalse isikutunnistuse vormi, tehnilise kirjelduse ja digitaalsele isikutunnistusele kantavate andmete loetelu kehtestamine. Vabariigi Valitsuse määrus nr 120, 26. august 2010. – RT I 2010, 61, 422; RT I, 28.11.2014, 11.
38. Digitaalseks isiku tõendamiseks ettenähtud dokumendi andmekandja tehnilised nõuded. Siseministri määrus nr 36, 12. august 2010. – RT I 2010, 66, 495 – RT I, 23.12.2010, 5.
39. Dokumendi taotleja isiku tuvastamise ja isikusamasuse kontrollimise kord. Siseministri määrus nr 25, 10. juuli 2009. – RTL 2009, 57, 836 – RT I, 23.12.2010, 5.
40. Eesti Vabariigi põhiseadus. 28. juuni 1992. – RT 1992, 26, 349; RT I, 27.04.2011, 1.
41. Eesti Vabariigi põhiseaduse täiendamise seadus. 14. september 2003. – RT I 2003, 64, 429.
42. Eesti Vabariigi välja antava elamisloakaardi vormi ja tehnilise kirjelduse ning elamisloakaardile kantavate andmete loetelu kehtestamine ja elamisloakaardile kantavate digitaalsete andmete kehtivusaja määramine. Vabariigi Valitsuse määrus nr 170, 09. detsember 2010. – RT I 17.12.2010, 3; RT I, 14.10.2014, 3.
43. Infosüsteemide andmevahetuskiht. Vabariigi Valitsuse määrus nr 78, 24. aprill 2008. – RT I 2008, 18, 129; RT I, 28.11.2014, 11.
44. Isikutunnistuse vormi ja tehnilise kirjelduse ning isikutunnistusele kantavate andmete loetelu kehtestamine ja isikutunnistusele kantavate digitaalsete andmete kehtivusaja määramine. Vabariigi Valitsuse määrus nr 169, 09. detsember 2010. – RT I, 17.12.2010, 2; RT I, 09.08.2011, 1.
45. Isikut tõendavate dokumentide seadus. 15. veebruar 1999. – RT I 1999, 25, 365; RT I, 23.03.2015, 1.
46. Isikut tõendavate dokumentide andmekogu pidamise põhimäärus. Vabariigi Valitsuse määrus nr 109, 03. juuli 2008. – RT I 2008, 31, 195 – RT I, 28.11.2014, 11.
47. Pagulasseisundi konventsiooni ja 31. jaanuari 1967. aasta pagulasseisundi protokolliga ühinemise seadus. 19. veebruar 1997. – RT II 1997, 6, 26.
48. Rahapesu ja terrorismi rahastamise tõkestamise seadus. 19. detsember 2007. – RT I 2008, 3, 21; RT I, 19.03.2015, 4.
49. Rahvastikuregistri seadus. 31. mai 2000. – RT I 2000, 50, 317; RT I, 29.06.2014, 109.
50. Riigi Infosüsteemide Ameti põhimäärus. Majandus- ja Kommunikatsiooniministri määrus nr 28, 25. aprill 2011. – RT I, 28.04.2011, 1; RT I, 27.02.2015, 5.
51. Sertifitseerimise riikliku registri asutamine ja pidamise põhimäärus. Vabariigi Valitsuse määrus nr 416, 12. detsember 2000. – RT I 2009, 63, 413.
52. Vabariigi Valitsuse korraldus nr 509 „Eesti infoühiskonna arengukava 2020“ ja selle

rakendusplaani aastateks 2014–2015 heakskiitmine. 18. november 2013. – RT III, 19.11.2013, 14.

53. Välismaalasele rahvusvahelise kaitse andmise seadus. 14. detsember 2005. – RT I 2006, 2, 3; RT I, 23.03.2015, 1.

Kasutatud kohtupraktika

54. EKo, 05.02.1963, 26/62, *Van Gend en Loos*. Arvutivõrgus: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=87120&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2399729, 24.04.2015.

Avaldamata allikad

55. Euroopa Komisjoni rakendusotsuse eelnõu 14. aprillist 2015 Euroopa Parlamendi ja Nõukogu määruse (EL) nr 910/2014 artiklite 8 ja 9 lg 1 järgi. – Lisas 1.

Muud allikad

56. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee of the Regions. Action plan for the implementation of the legal framework for electronic public procurement. Commission of the European Communities. Brussels, 13.12.2004. Online: http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/actionplan/actionplan_en.pdf, 28.03.2015.
57. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme. Brussels, 20.4.2010. COM(2010) 171 final. Online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:en:PDF, 23.04.2015.
58. Eesti Euroopa Liidu poliitika 2011-2015. Arvutivõrgus: https://www.riigikantselei.ee/valitsus/valitsus/et/riigikantselei/euroopa/Eesti%20EL%20poliitika_EST.pdf, 26.02.2015.
59. Eesti infoühiskonna arengukava 2020. Majandus ja Kommunikatsiooniministeerium 2013. Arvutivõrgus: http://infoyhiskond.eesti.ee/files/Infoyhiskonna_arengukava_2020_f.pdf, 23.04.2015.
60. Eesti Politsei- ja Piirivalveamet. Mobiil-ID taotlemine. Arvutivõrgus: https://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/mobiil-id/, 24.04.2015.

61. Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Res Publica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta. 08.04.2015. Arvutivõrgus: https://valitsus.ee/sites/default/files/content-editors/failid/re-sde-irl-valitsusliidu-lepe-2015.pdf, 15.04.2015.
62. eIDAS Private Sector Engagement High Level Event "eID: a key to business growth and innovation". Online: https://ec.europa.eu/digital-agenda/en/news/eidas-private-sector-engagement-high-level-event, 24.04.2015.
63. eIDAS Private Sector Engagement High Level Event "eID: emerging business cases". Online: https://ec.europa.eu/digital-agenda/en/news/eidas-private-sector-engagement-high-level-event-eid-emerging-business-cases, 24.04.2015.
64. Elektrooniline identiteet. Riigi Infosüsteemi Amet. Arvutivõrgus: https://www.ria.ee/elektrooniline-identiteet/, 14.03.2015.
65. Elektrooniliste isikutuvastuste statistika. Arvutivõrgus: http://www.id.ee/, 21.04.2015.
66. EUROPE 2020. A strategy for smart, sustainable and inclusive growth. COM(2010) 2020 final. Pp 7-35. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF, 23.04.2015.
67. Europan Commission. IDABC. eID Interoperability for PEGS. Online: http://ec.europa.eu/idabc/en/document/6484.html, 08.04.2015.
68. European Commission MEMO "Q&A: Electronic Identification and Trust Services (eIDAS) Regulation". Brussels, 14th October 2014. Online: http://europa.eu/rapid/press-release_MEMO-14-586_en.htm, 18.04.2015.
69. European Commission. Internal Market. Services Directive "Points of single contact". Online: http://ec.europa.eu/internal_market/eu-go/index_en.htm#ee, 11.04.2015.
70. European Network and Information Security Agency. Study: Mapping security services to authentication levels, p. 1-34. Online: https://www.eid-stork.eu/dmdocuments/public/mapping.pdf, 08.04.2015.
71. Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide komiteele. 21. sajandi Euroopa ühtne turg. Brüssel 20.11.2007. KOM(2007) 724 lõplik. Arvutivõrgus: http://ec.europa.eu/transparency/regdoc/rep/1/2007/ET/1-2007-724-ET-F1-1.Pdf, 23.04.2015.
72. Isikut tõendavate dokumentide seaduse, konsulaarseaduse, karistusseadustiku, riigilõivuseaduse, välismaalaste seaduse ja kodakondsuse seaduse muutmise seadus 395

SE seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/df3dd438-72e6-bdd9-acb3-f3aac7d2f025/Isikut-t%C3%B5endavate-dokumentide-seaduse,-konsulaarseaduse,-karistusseadustiku,-riigil%C3%B5ivuseaduse,-v%C3%A4lismaalaste-seaduse-ja-kodakondsuse-seaduse-muutmise-seadus/, 30.04.2015.

73. Isikut tõendavate dokumentide seaduse ja teiste seaduste muutmise seaduse eelnõu seletuskiri, 844 SE II.
Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/5422b8d0-33ed-7890-b56a-7452b83d8b56/Isikut-t%C3%B5endavate-dokumentide-seaduse-ja-teiste-seaduste-muutmise-seadus/, 30.04.2015.
74. Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide komiteele. Euroopa digitaalne tegevuskava. Euroopa Komisjon. Brüssel 19.5.2010, KOM(2010)245 lõplik. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245, 28.03.2015.
75. Langemets, M. *et al* (toim). Eesti keele seletav sõnaraamat. „Eesti kirjakeele seletussõnaraamatu" 2., täiendatud ja parandatud trükk. Eesti Keele Sihtasutus. Tallinn 2009. Veebiväljaanne. Arvutivõrgus: http://www.eki.ee/dict/ekss/ekss.html, 28.02.2015.
76. Ministerial Declaration. Approved unanimously on 24 November 2005, Manchester, United Kingdom. Arvutivõrgus: http://www.umic.pt/images/stories/noticias/051124declaration.pdf, 28.03.2015.
77. Ministerial Declaration. approved unanimously in Lisbon, Portugal on 19 September 2007. Arvutivõrgus: http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=392, 28.03.2015.
78. Mitteresidentidele digitaalse isikutunnistuse väljaandmine: e-residentsuse loomine. Kontseptsioon. Arvutivõrgus: https://www.siseministeerium.ee/public/e-residendi_digi_id_Lisa_1_kontseptsioon.pdf, 28.03.2015.
79. Opinion of the Economic and Social Committee on the "Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market". On 23 April 1999 the Council decided to consult the Economic and Social Committee, under Article 100a of the Treaty establishing the European Community, on the above-mentioned proposal. Official Journal C 169, 16/06/1999. Online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51999AC0457, 23.04.2015.
80. Proposal for a European Parliament and Council Directive on a common framework for electronic signatures (98/C 325/04) (Text with EEA relevance) COM(1998) 297 final -

98/0191(COD). (Submitted by the Commission on 16 June 1998). Official Journal C 325, 23/10/1998. Online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.1998.325.01.0005.01.ENG, 24.04.2015.

81. Riigi Infosüsteemide Amet. Elektrooniline identiteet. Arvutivõrgus: https://www.ria.ee/elektrooniline-identiteet/, 14.03.2015.
82. RISO. Teiste riikide eID hindamise põhimõtted. Arvutivõrgus: http://www.riso.ee/et/koosvoime/identiteet/teiste-riikide-serdid.html, 08.04.2015.
83. Sertifitseerimise register. Teiste riikide eID-d. Arvutivõrgus: https://sr.riik.ee/et/usaldusnimekiri/TeisedRiigid.html, 16.04.2015.
84. Sertifitseerimiskeskuse sertifitseerimispõhimõtted (*Certification Practice Statement*), versioon 2.5. Peatükid 4-6. Arvutivõrgus: https://www.sk.ee/repositoorium/CPS/, 13.04.2015.
85. SK uudis: "Eesti ja Soome peaministrid digiallkirjastasid riikidevahelise IKT koostöömemorandumi". Arvutivõrgus: http://www.id.ee/?id=36540, 13.03.2015.
86. SK tühistusnimekiri. Arvutivõrgus: https://sk.ee/repositoorium/CRL/CRL, 13.04.2015.
87. STORK. Online: https://www.eid-stork.eu/, 08.04.2015.
88. STORK Pilot 4. Piiriülese e-edastuse projekt – turvalise dokumentide vahetamise mehhanismi arendamine. Arvutivõrgus: https://www.eid-stork.eu/pilots/pilot4_EE.htm, 28.02.2015.
89. http://sr.riik.ee/et/sp.html, 22.03.2015.
90. http://et.wikipedia.org/wiki/Eesti_ID-kaart, 20.03.2015.

Non-paper (5) on determining levels of assurance for electronic identification schemes being notified to the Commission pursuant to Articles 8 and 9(1)

ACTION

The expert group is requested to provide its views on the draft text below.

INTRODUCTION

This non-paper is an updated version of the previous non-paper, prepared also for the April expert group meeting. It includes the revision of point 2.1.2 of the Annex, and it takes into account the preliminary input of the Legal Service of the Commission.

This non-paper reflects in its Annex how the exercise of the implementing powers granted by Article 8(3) of the Regulation on electronic identification and trust services for electronic transactions in the internal market should be done taking into account international standards (in particular ISO 29115) and results of Union-funded Large Scale Pilots (in particular STORK) as provided in recital 16 of the Regulation.

The draft implementing act in the Annex builds on the input of the drafting group and takes into account discussions in eIDAS expert group and written contributions by Member States experts submitted via CIRCABC.

As requested by the experts, this version shows the changes compared to the previous non-paper prepared also for the April expert group meeting.

We shall emphasize that the text attached to this non-paper is a preliminary draft and does not constitute an official draft of the Commission; it serves the sole purpose of reference point for discussion in the eIDAS Expert Group. However, as the previous version has already been discussed by the expert group and the experts' contributions were taken into account, we do not foresee significant changes in most parts.

Annex

DRAFT

[…]

Whereas:

Article 8 of ~~the~~ Regulation (EU) No 910/2014 provides that an electronic identification scheme notified pursuant to Article 9(1) ~~shall~~needs to specify assurance levels low, substantial and high for electronic identification means issued under that scheme.

Determining the minimum technical specifications, standards and procedures is essential in order to ensure common understanding of the details of the assurance levels and to ensure interoperability when mapping the national assurance levels of notified electronic identification schemes to the assurance levels under Article 8 as provided by Article 12(4)(b) of ~~the~~ Regulation (EU) No 910/2014.

International standard ISO/IEC 29115 has been taken into account for the specifications and procedures set out in this implementing act as being the only international standard available in the domain of assurance levels for electronic identification means. However, additional technical specifications and procedures set out in ~~the~~ Regulation (EU) No 910/2014 in relation to assurance levels of the electronic identification means should also be complied with. In particular identity proofing and verification requirements need to be met, as well as recognising the differences between Member State identity arrangements. Therefore the Annex while building on this international standard ~~does~~should not establish any direct reference to ISO/IEC 29115.

The definitions used to specify the terms and concepts in the Annex, have been developed as an outcome based approach as being the most appropriate. They take into account the aim of ~~the~~ Regulation (EU) No 910/2014 in relation to assurance levels of the electronic identification means. Therefore, Large-Scale Pilot STORK, including specifications developed by it, and the definitions and concepts in ISO/IEC 29115 ~~have been~~should be taken into the utmost account when establishing the specifications and procedures set out in this implementing act.

There are authentication factors such as shared secrets, tokens and physical attributes. The authentication factors belong to different factor categories. The usage of more authentication factors, especially where they are from different factor categories increases the security of the authentication process.

The importance of information security and service management systems ~~is~~should be recognised, as ~~is~~should the importance of the employment of recognised methodologies and adoption of principles found in standards such as the ISO/IEC 27000 and the ISO/IEC 20000 series.

Good practices in relation to assurance levels in the Member States ~~have~~should also be taken into account.

IT security certification based on international standards is an important tool for verifying the security compliance of products with the security requirements of the implementing act.

[…]

Article 1

~~**Subject matter**~~

~~Technical specifications and procedures specifying assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme are laid down in the Annex.~~

~~**Article 2**~~

~~**Assurance levels of electronic identification means issued under notified electronic identification scheme**~~

1. Assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme shall be determined ~~by~~with reference to the specifications and procedures set out in the Annex.

2. The technical specifications and procedures set out in the Annex shall be used to specify the ~~level of~~ assurance level of the electronic identification means issued under a notified electronic identification scheme by determining the reliability and quality of following elements:

(a) enrolment set out in section 2.1 ~~in~~of the Annex to this Regulation pursuant to Article 8(3~~) point ()~~(a) of ~~the~~ Regulation (EU) No 910/2014;

(b) electronic identification means management set out in section 2.2 ~~in~~of the Annex to this Regulation pursuant to Article 8(3~~) points ()~~(b) and (f) of ~~the~~ Regulation (EU) No 910/2014;

(c) authentication set out in section 2.3 ~~in~~of the Annex to this Regulation pursuant to Article 8(3~~) point ()~~(c) of ~~the~~ Regulation (EU) No 910/2014;

(d) management and organisation set out in section 2.4 ~~in~~of the Annex to this Regulation pursuant to Article 8(3~~) points ()~~(d) and (e) of ~~the~~ Regulation (EU) No 910/2014.

3. When the electronic identification means issued under a notified electronic identification

scheme meets a requirement listed in a higher assurance level then it ~~is~~shall be presumed to fulfil the equivalent requirement of a lower assurance level.

4. Unless otherwise stated in the relevant part of the Annex, all elements listed in the Annex for a particular ~~level of~~ assurance level of the electronic identification means issued under a notified electronic identification scheme shall be met in order to ~~achieve/~~match the claimed ~~level of~~ assurance level.

Article ~~3~~2

~~**Entry into force**~~

This ~~decision~~Regulation shall apply from ….~~**Article 4**~~

~~**Addressees**~~

Annex

Technical specifications and procedures for assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme

1. Applicable definitions

For the purposes of this Annex, the following definitions shall apply:

(1) 'authoritative source' means any source that can be relied upon to provide accurate data, information and/or documents that can be used to prove identity;

(2) 'authentication factor' means a ~~shared secret, token and/or physical attribute~~factor confirmed as being bound to a subject, which falls into any of the following categories:

(a) 'possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it;

(b) 'knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it;

(c) 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person ~~possess,~~ and which the subject is required to demonstrate ~~that they have that physical attribute~~possession;

(3) 'dynamic authentication' means an electronic process using cryptography or other techniques to create an authenticator which changes with each authentication between a claimant and a verifier;

(4) 'authenticator' means a means of creating on demand ~~[a one time only]~~an electronic proof which is different on each occasion that the claimant is in control and in possession of the credential being used for authentication.

(5) 'information security management system' means a set of processes and procedures designed to manage ~~information security related risks~~ to acceptable levels risks related to information security.

2. Technical specifications and procedures

The elements of technical specifications and procedures outlined in this Annex shall be used to determine how the requirements and criteria of Article 8 of ~~the~~ Regulation (EU) No 910/2014 shall be applied for electronic identification means issued under an electronic identification scheme.

2.1 Enrolment

2.1.1 Application and registration

Assurance level	Elements needed
Low	- Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. - Ensure the applicant is aware of recommended security precautions related to the electronic identification means. - Collect the relevant identity data required for identity proofing~~.~~ and verification.
Substantial	- Same as ~~Low~~level low.
High	- Same as ~~Low~~level low.

2.1.2 Identity proofing and verification (natural person)

Assurance level	Elements needed
Low	All of the elements below have to be met: 1. The person can reasonably be assumed to be in possession of nationally recognised evidence representing the claimed identity. 2. The evidence appears to be valid. 3. The claimed identity is known to exist by authoritative source(s) and is not known to be deceased. 4. The applicant is identified by using information obtained from an authoritative source.
Substantial	~~Same as point 3 of level~~Level low plus one of the alternatives below has to be met: 1. The person has been verified to be in possession of nationally recognised evidence representing the claimed identity~~.~~ ~~The~~ and the evidence is checked to determine it is genuine or valid according to an authoritative source. or 2. Where a nationally issued identity document is presented during a registration process in the Member State where the document was issued and ~~which~~the document appears to relate to the person presenting it and it appears genuine, subject to a check that it has not been reported lost, stolen suspended or revoked it may be regarded as the authoritative source itself. or 3. Where procedures used previously by an entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the corresponding assurance level then the registration authority for the issuance of the electronic identification means need

	not to repeat those earlier processes, provided that such equivalent assurance is confirmed by a conformity assessment body ~~according~~referred to ~~point 13 of~~in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council[210] or equivalent. or 4. Where, save for renewal or replacement, electronic identification means are issued on the basis of a notified electronic identification means having the same or a higher ~~level of~~ assurance level it is not required to repeat the registration processes. Where the electronic identification means serving as the basis has not been notified, the equivalent or higher assurance must be confirmed by a conformity assessment body ~~according~~referred to ~~point 13 of~~in Article 2(13) of Regulation (EC) No 765/2008 or equivalent.
High	~~Same as points 3-5~~One of ~~level~~the alternatives 1. or 2. below has to be met: 1. Level substantial plus one of the alternatives (a. b or c) below has to be met: a. Where the person has been verified to be in possession of nationally recognised photo or biometric identification evidence representing the claimed identity, the evidence is checked to determine that it is both genuine and valid according to an authoritative source; ~~the claimed identity is known to exist by authoritative source(s) and is not known to be deceased;~~ and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source for the presented evidence. or b. Same as points 3 of level substantial, but corresponding to level high plus: checks are made that the results of this previous procedure remain valid or c. Same as point 4 of level substantial plus:

[210] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

	checks are made that any previously issued electronic identification means serving as the basis for the issuance is not known to be lost, stolen, suspended or revoked. OR ~~1.~~ Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level of the Member State of the registration authority to obtain such recognised photo or biometric identification evidence shall be applied. 2. ~~Checks are made that any previously issued electronic identification means serving as the basis for the issuance is not known to be lost, stolen, suspended or revoked.~~

2.1.3 Identity proofing and verification (legal person)

Assurance level	Elements Needed
Low	- The claimed identity of the legal person is demonstrated on the basis of nationally recognised evidence. - The evidence appears to be valid according to an authoritative source~~;~~ where inclusion of a legal person in the authoritative source is voluntary and is regulated by an agreement between the legal person and the authoritative source. - The legal person is not known to be in a status that would prevent it from acting as that legal person.
Substantial	- The claimed identity of the legal person is demonstrated on the basis of nationally recognised evidence, which includes at least the legal person's name, legal form, and (if applicable to the legal person) its registration number. - The evidence is determined to be valid according to an authoritative source ~~and~~, where inclusion of a legal person in the authoritative source is required for the legal person to operate within its sector and is regulated by a nationally recognised regulatory body. - The legal person is not known to be in a status that would prevent it acting as that legal person. - Where additional electronic identification means are issued by the same issuer, it is not needed to repeat the processes of the identity proofing and verification described provided that all the steps have been undertaken by the registration authority before the issuance of the first electronic identification means and the issuance of subsequent means is based on those steps previously undertaken
High	- The claimed identity of the legal person is demonstrated on the basis of nationally recognised evidence, which includes at least the legal person's name, legal form, and at least one unique identifier. - The evidence is determined to be valid according to an authoritative source

	and where inclusion of legal person in the authoritative source is required by national law and is regulated by a ~~government or government appointed body~~public sector body as referred to in Article 3(7) of Regulation (EU) No 910/2014. - The legal person is not known to be in a status that would prevent it from acting as that legal person. - Where the procedures ~~used~~ at the national level of the ~~member state~~Member State of the registration authority are used that also include the above requirements then the registration authority need not to repeat those processes, provided that such equivalent assurance is confirmed by a conformity assessment body ~~according~~referred to ~~point 13 of~~in Article 2(13) of Regulation (EC) No 765/2008 or equivalent. - Where additional electronic identification means are issued by the same issuer, it is not needed to repeat the processes of the identity proofing and verification described provided that all the steps have been undertaken by the registration authority before the issuance of the first electronic identification means and the issuance of subsequent means is based on those steps previously undertaken.

2.1.4 Binding between natural persons and legal persons

Whenever applicable, for binding between a natural person and a legal person:

i) The authoritative source ~~is~~shall be responsible for administering the life-cycle of a binding (e.g. activation, suspension, renewal, revocation) according to nationally recognised procedures.

ii) The administration of the binding may be delegated by the identified natural person to another ~~in~~ on the basis of nationally recognised procedures; however the accountability remains with the natural person that was identified in accordance with these procedures.

iii) Binding between a natural person and a legal person shall be done in the following manner:

Assurance level	**Elements Needed**
Low	- The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above. - The binding between the natural person and the legal person has been established on the basis of nationally recognised procedures. - The natural person is not known to be in a status that would prevent ~~them~~that person from acting on behalf of the legal person.
Substantial	- The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high. - The binding between the natural person and the legal person has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source. - The binding between the natural person and the legal person has been

	verified on the basis of information from an authoritative source. - The natural person is not known to be in a status that would prevent ~~them~~that person from acting on behalf of the legal person.
High	- The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high. - The binding between the natural person and the legal person has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source. - The binding between the natural person and the legal person has been verified on the basis of a unique identifier representing the legal person and information uniquely representing the natural person from an authoritative source. - The natural person is not known to be in a status that would prevent ~~them~~that person from acting on behalf of the legal person.

2.2. Electronic identification means management

2.2.1 Electronic identification means characteristics and design

Assurance level	Elements needed
Low	- The electronic identification means shall ~~be comprised of~~utilise at least one authentication factor. - The electronic identification means shall be designed so that it can be assumed to be used only if under the control of the ~~applicant.~~subject to whom it belongs.
Substantial	- The electronic identification means shall ~~be comprised of~~utilise at least two authentication factors from different authentication factor categories. - The electronic identification means shall be designed so that it can reasonably be assumed to be used only if under the control of the ~~applicant.~~subject to whom it belongs..
High	- The electronic identification means shall ~~be comprised of~~utilise at least two authentication factors from different authentication factor categories and protect the electronic identification means against duplication and tampering. - The electronic identification means shall be designed so that it can be reliably protected by the ~~legitimate holder~~subject to whom it belongs against use by others.

2.2.2 Issuance, delivery and activation

Assurance level	Elements needed
Low	- After issuance, the electronic identification means shall be delivered via a mechanism by which it can be assumed to reach only the ~~applicant.~~intended subject.
Substantial	- After issuance, the electronic identification means shall be delivered via a mechanism by which it can be reasonably assumed that it is delivered only into the possession of the ~~applicant~~subject to whom it belongs
High	-The activation process verifies that the electronic identification means was delivered only into the possession of the ~~applicant~~subject to whom it belongs.

2.2.3 Suspension, revocation and reactivation

Assurance level	Elements needed
Low	- It shall be possible to suspend and/or revoke an electronic identification means in a timely manner and effectively. - There shall be measures taken to prevent unauthorised suspension, revocation and/or reactivation. - Reactivation shall take place only if the same assurance requirements as initially established continue to be met.
Substantial	- Same as ~~Low~~level low.
High	- Same as ~~Low~~level low.

2.2.4 Renewal and replacement

Assurance level	Elements needed
Low	- Renewal or replacement shall meet the same assurance requirements as initial establishment or be based on a valid electronic identification means of the same, or higher, assurance level.
Substantial	- Same as ~~Low~~level low.
High	- Same as ~~Low~~level low, plus the following: • Where renewal or replacement is based on a valid electronic identification means, the identity data shall be verified with an authoritative source.

2.3. Authentication

This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls ~~are~~shall be understood to be commensurate to the risks at the given level.

2.3.1 Authentication mechanism

The following table represents the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.

Assurance level	Elements needed
Low	- The release of ~~identity information~~person identification data shall be preceded by reliable verification of the electronic identification means and its validity. - Where person identification data is stored as part of the authentication mechanism, that information shall be secured in order to protect against loss and compromise including analysis offline. - The authentication mechanism shall implement security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.

Substantial	- Same as ~~Low~~level low, plus the following: ● The release of identity information shall be preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process. • The authentication mechanism shall implement security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
High	- Same as ~~Substantial~~level substantial, plus the following: • The authentication mechanism shall implement security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

2.4. Management and organisation

All participants involved in cross-border operations ~~should~~shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies in the respective Member States that effective practices are in place. Throughout section 2.4, all controls ~~are to~~shall be understood as commensurate to the risks at the given level.

2.4.1 General provisions

Assurance level	Elements needed
Low	- Any provider delivering any operational service covered by this document shall be a public authority or a legal entity recognised as such by national law of ~~an EU~~ Member State, with an established organisation and fully operational in all parts relevant for the providing of the services. - All providers shall comply with any legal requirements incumbent on them in connection with operation and delivery of the service including, but not limited to, the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long. - The entity providing the service shall be able to demonstrate the ability to assume the risk of liability for damages, as well as having sufficient financial resources for continued operations and providing of the services. - The entity providing the service ~~is~~shall be responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the entity itself had performed the duties. - Electronic identification schemes not constituted by national law shall have an effective termination plan that includes orderly discontinuations of service or continuation by another provider, informing relevant authorities and end users and including details of how records are to be protected, retained and destroyed in compliance with policy.
Substantial	- Same as ~~Low~~level low.
High	- Same as ~~Low~~level low.

2.4.2 Published notices and user information

Assurance level	Elements needed
Low	- There shall be a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy. - Appropriate policy and procedures shall be in place that ~~provides~~provide for users of or subscribers to the service to be notified in a timely and reliable fashion of any changes to the service definition and any applicable terms, conditions, and privacy policy for the specified service. - Appropriate policy and procedures shall be in place that provides for full and correct responses to requests for information.
Substantial	- Same as ~~Low~~level low.
High	- Same as ~~Low~~level low.

2.4.3 Information security management

Assurance level	Elements needed
Low	- There shall be effective Information Security Management Systems (ISMS) for the management and control of information security risks.
Substantial	- The ISMS shall adhere to proven standards or principles for the management and control of information security risks.
High	- Same as ~~Substantial~~level substantial.

2.4.4 Record keeping

Assurance level	Elements needed
Low	- Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention. - Retain and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention is permitted by national law or other regulation, after which the records shall be securely destroyed.
Substantial	- Same as ~~Low~~level low.
High	- Same as ~~Low~~level low.

2.4.5 Facilities and staff

The following table represents the requirements with respect to facilities and staff and subcontractors, if applicable, who undertake duties covered by this ~~implementing act [type of the act in the later stage]~~.Regulation. Compliance to each of the requirements shall be proportionate to the level of risk associated with the assurance level provided.

Assurance level	Elements needed
Low	- There shall be processes that ensure staff and subcontractors are sufficiently

	trained, qualified and experienced in the skills needed to execute the roles they fulfil. - There shall be sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures. - Facilities used for providing the service shall be continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service. - Facilities used for providing the service shall limit access to areas holding or processing personal, cryptographic or other sensitive information to authorised staff or subcontractors.
Substantial	- Same as ~~Low~~level low.
High	- Same as ~~Low~~level low.

2.4.6 Technical controls

Assurance level	Elements needed
Low	- There shall be proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed. - Electronic communication channels used to exchange personal or sensitive information shall be protected against eavesdropping, manipulation and replay. - Access to sensitive cryptographic material used for issuing electronic identification means and authentication shall be restricted to the roles and applications strictly requiring access, never stored in plaintext in persistent storage. - Procedures shall exist to ensure that security is maintained over time and ability to respond to changes in risk levels, incidents and security breaches. - All media containing personal, cryptographic or other sensitive information shall be stored, transported and disposed of in a safe and secure manner.
Substantial	- Same as ~~Low~~level low, plus the following: • Sensitive cryptographic material used for issuing electronic identification means and authentication held in persistent storage shall be protected from tampering.
High	- Same as ~~Substantial~~level substantial.

2.4.7 Compliance and audit

Assurance level	Elements needed
Low	-There shall be periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.
Substantial	- There shall be periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.
High	- There shall be periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy. - Where a scheme is directly managed by a government body, it shall be audited in accordance with the national law.