TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Tarkvarateaduse instituut

Kristel Merilain 155604IABB

EESTIS KASUTATAVATE ELEKTROONILISE IDENTITEEDI VAHENDITE ÄRI- JA RISKIANALÜÜS

bakalaureusetöö

Juhendaja: Karin Rava
MSc. Eng

Kaasjuhendaja: Annika Kluge
Riigi Infosüsteemi Ameti eID valdkonna projektijuht

Tallinn 2018

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Kristel Merilain

21.05.2018

Annotatsioon

Lõputöö eesmärgiks on anda ülevaade elektroonilise identiteedi (eID) olemusest ning teostada elektroonilise identiteedi vahendite äri- ja riskianalüüs.

Olulisemad probleemid, mida antud töös käsitletakse, on seotud elektroonilise identiteedi vahendite võimalike ohtude ja riskidega.

Töö kõige olulisemateks tulemusteks on elektroonilise identiteedi vahendite ja kasutusalade ülevaade, elektroonilise identiteedi vahendite võrdlemise tulem kasutades SWOT- ja riskianalüüsi ning elektroonilise identiteedi vahendite ja kasutusalade populaarsuse hinnang kasutajate seas internetiküsitluse tulemuste põhjal.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 55 leheküljel, 8 peatükki, 6 joonist, 6 tabelit.

Abstract

Business and Risk Analysis of Electronic Identity Tools Used in Estonia

The aim of this thesis is to provide an overview of the essence of electronic identity and to carry out business and risk analysis of electronic identity tools.

The main problems described in this thesis are related to the potential threats and risks of electronic identity.

The main results of this thesis are the overview of electronic identity tools and uses, comparing different types of electronic identity tools using SWOT and risk analysis and the popularity of electronic identity tools and uses among users based on the results of an online survey.

The thesis is in Estonian and contains 55 pages of text, 8 chapters, 6 figures, 6 tables.

Lühendite ja mõistete sõnastik

eID	Elektrooniline identiteet
eIDAS	*electronic IDentification, Authentication and trust Services* [1]
OCSP	*Online Certificate Status Protocol* [2]. Teenus mis kontrollib kas kasutaja sertifikaat hetkel kehtib [3].
DDOC	Digitaalselt allkirjastatud faili formaat, mis oli kasutusel 2015. aastani [4].
BDOC	Eestis alates 2015. aastast kasutusel olev digitaalselt allkirjastatud faili formaat, selles formaadis on allkiri ajamärgendiga [4].
ASiC-E	Rahvusvaheliselt tunnustatud digitaalselt allkirjastatud faili formaat, millel on allkiri ajatempliga [4].
TeRa	Tembeldamise Rakendus, see on mõeldud aegunud digitaalselt allkirjastatud vana failiformaadi .ddoc ületembeldamiseks. Ületembeldamise käigus lisatakse ajatempel ning tehakse uus ASiC-E konteiner [5].
CDOC	Krüpteeritud faili formaat, mida kasutatakse DigiDoc vormingus failide eristamiseks [6].
PKI	*Public Key Infrastructure* ehk Avaliku võtme infrastruktuur. PKI on teenuste kogum, mille vahendusel saavad inimesed või seadmed turvaliselt suhelda infotehnoloogilises keskkonnas [7].

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Elektrooniline identiteet (edaspidi eID) on elektroonilises keskkonnas kasutusel olev digitaalne isikutuvastusvahend [8]. eID on pidevas arengus, mistõttu on loodud palju erinevaid eID vahendeid ja võimalusi erinevateks kasutusaladeks. Seniste analüüside tulemusena ei ole selgelt välja toodud Eesti elektroonilise identiteedi vahendite erinevusi, ohtusid ja võimalusi. Lisaks võib väita, et varasemalt pole uuritud kasutajate arvamusi erinevate elektroonilise identiteedi vahendite ja kasutusalade kohta. Antud töö püüab seda puudust kõrvaldada. Lõputöös antakse ülevaade erinevatest elektroonilise identiteedi vahenditest, nende võimalikest kasutusaladest ning analüüsitakse elektroonilise identiteedi vahendite võimalusi, ohtusid ning riske. Antud töö annab tavakasutajale hea ülevaate elektroonilise identiteedi olemusest ning võimaldab kasutajal leida endale sobivaim eID vahend, võttes arvesse analüüsi tulemit.

Lõputöö eesmärgid on järgmised:

1. Selgitada, mis on elektrooniline identiteet ning kuidas selle kasutamine on Eestis alguse saanud ning levinud, anda ülevaade elektroonilise identiteedi vahenditest ning kasutusaladest.

2. Teostada erinevate elektroonilise identiteedi vahendite ja nende kasutusalade analüüs:

    1. Selgitada välja nende populaarsus lõppkasutajate seas,

    2. määratleda, millised on nendega kaasnevad riskid,

    3. tuvastada nendega kaasnevad võimalused.

Töö teises peatükis defineeritakse elektroonilise identiteedi olemus ning antakse ülevaade, kuidas sai eID Eestis alguse. Töö kolmandas peatükis tutvustatakse mõningaid elektroonilise identiteedi vahendeid Eestis: ID-kaart, Mobiil-ID, Smart-ID ja Digi-ID. Töö neljandas peatükis antakse ülevaade erinevatest võimalustest, kuidas on võimalik elektroonilist identiteeti Eestis kasutada. Töö viiendas peatükis antakse ülevaade,

milliseid erinevaid vahendeid mujal maailmas kasutatakse. Töö kuuendas peatükis selgitatakse, milliste metoodikate alusel toimub äri- ja riskianalüüs. Töö seitsmendas peatükis analüüsitakse erinevaid eID vahendeid kasutades SWOT - analüüsi, riskianalüüsi ning uuritakse erinevate vahendite populaarsust kasutajate seas.

2 Elektrooniline identiteet ehk eID

Elektrooniline identiteet (lühendatult eID) on digitaalne isikutuvastusvahend, mis on kasutusel elektroonilises keskkonnas ning see on otseselt seotud füüsilise isikuga [8]. Eestis on elektroonilise identiteedi vahenditeks ID-kaart, Digi-ID, e-residendi Digi-ID, elamisloakaart, välisdiplomaadi kaart, Smart-ID ning Mobiil-ID [3].

Elektrooniline identiteet sai Eestis alguse 1999. aastal, kui Euroopa Liidus võeti vastu direktiiv *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures* [9] ehk *Euroopa Parlamendi ja Nõukogu Direktiiv 1999/93/EÜ, 13. detsember 1999, elektroonilisi allkirju käsitleva ühenduse raamistiku kohta* [10]. Direktiiv sätestas üldised nõuded allkirja andmise vahenditele ja sertifikaatidele [11]. Siseriiklikul tasandil jõustus digitaalallkirja seadus 15. detsembril 2000 [12]. Digitaalallkirja seadus kirjeldab Eestis olevat digitaalallkirja mõistet ning sellega seotud tegevusi ja teenuseid [13].

2001. aastal asutati AS Sertifitseerimiskeskus, et pakkuda digitaalse allkirja kasutusse võtmiseks vajalikku sertifitseerimisteenust, mis võimaldab kodanikel oma igapäevaelus kasutada turvalist ja tõendatud elektroonilist kommunikatsiooni [14].

Sertifitseerimisteenus sisaldab endas digitaalse allkirja andmiseks vajalike sertifikaatide väljaandmist, sertifikaatide alusel antud digitaalsete allkirjade kontrollimist ning sertifikaatide kehtivuse peatamist, kehtivuse peatatuse lõpetamist ja kehtetuks tunnistamise menetlemist [15].

14. detsember 2001 allkirjastasid siseminister ja AS Sertifitseerimiskeskuse juhataja lepingu, mille kohaselt hakkas Sertifitseerimiskeskus osutama siseministeeriumile sertifitseerimisteenust, mis on kooskõlas digitaalallkirja seadusega [16].

Alates 2002. aasta 3. oktoobrist said kõik soovijad tasuta alla laadida DigiDoc programmi, millega saab anda Eestis seaduslikult kehtivat digitaalset allkirja. Programmi said kasutada kõik, kellel oli olemas ID-kaart ja kaardilugeja ning arvuti õigesti seadistatud [17].

2016. aastal kehtima hakanud määrusega *Regulation (Eu) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC* [18] ehk *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* [19] (edaspidi eIDAS) tunnistati kehtetuks direktiiv 1999/93 EÜ. Määrus eIDAS koosneb kahest osast. Esimene osa sellest puudutab Euroopa Liidu liikmesriikide koostööd elektrooniliste isikutuvastusvahendite tunnustamisel ja hindamisel. Määrus määrab vahendite ja süsteemide usaldusväärsuse tasemed, mille põhjal saavad teenuse osutajad otsustada, millise tasemega vahendeid nad enda teenustes tunnustavad. Teine osa sellest puudutab tingimusi ja nõudeid erinevate usaldusteenuste osutamiseks. Usaldusteenuseid on vaja turvaliseks toimetamiseks digitaalses maailmas, näiteks digitaalsete allkirjade andmiseks ja nende kontrollimiseks ning veebisertifikaadid veebiturvalisuse tõstmiseks [20].

2016. aastal jõustus e-identimise ja e-tehingute usaldusteenuste seadus, millega kehtestati siseriiklikud alused e-identiteedi ja e-allkirjade sertifikaatide väljaandmiseks ja kasutamiseks. See seadus loodi Euroopa Liidu määruse eIDAS rakendamiseks. Sellega tunnistati kehtetuks 2016. aastani kehtinud digitaalallkirja seadus [21].

3 eID vahendid

Selles peatükis antakse ülevaade mõningatest elektroonilise identiteedi vahenditest, milleks on ID-kaart, Mobiil-ID, Smart-ID ja Digi-ID. Selles lõputöös ei anta ülevaadet elamisloakaardist, kuna see on funktsionaalse poole pealt sarnane ID-kaardiga, ning välisdiplomaadi kaardist, kuna sellel on vaid paarsada kasutajat. E-residendi Digi-ID ning Digi-ID on võetud üheks alapeatükiks kokku, kuna funktsionaalne pool on neil sama, erinev on vaid taotlemise ja väljastamise protsess ning tasu kaardi eest [3].

3.1 ID-kaart

ID-kaart on Eestis kohustuslik isikut tõendav dokument, mida saab kasutada ka elektrooniliseks isikutuvastamiseks, digitaalse allkirja andmiseks, andmete krüpteerimiseks, kliendikaardina ja läbipääsusüsteemides [22].

ID-kaarti saab taotleda Politsei- ja Piirivalveameti teenindustes, e-teeninduses, Eesti Vabariigi välisesindustes, postiga või e-postiga [23]. ID-kaardi kehtivusajaks on 5 aastat [24].

Koos ID-kaardiga väljastatakse koodiümbrik, milles on kirjas PIN-koodid, need on vajalikud ID-kaardi elektrooniliseks kasutamiseks: PIN1-kood on mõeldud isikutuvastuseks, PIN2-kood on mõeldud digitaalseks allkirjastamiseks ning PUK-kood on mõeldud lukustunud PIN-koodide avamiseks [25].

Selleks, et ID-kaarti saaks kasutada turvaliselt ka elektrooniliselt, kantakse kontaktkiibile isiku digitaalset tuvastamist võimaldav sertifikaat, digitaalselt allkirjastamist võimaldav sertifikaat ning nendes sertifikaatides sisalduvate avalikele võtmetele üheselt vastavad isiklikud võtmed ja andmefail [26].

ID-kaardi elektrooniliseks kasutamiseks on vaja ID-tarkvara, PIN-koode, kehtivaid sertifikaate, internetiühendusega arvutit ja kaardilugejat [27].

ID-kaarte hakati väljastama 2002. aastal [28]. Esimesteks ID-kaardi saajateks olid Arnold Rüütel ja Ingrid Rüütel [29].

Kuni 2007. aastani väljastatud ID-kaardid kehtisid 10 aastat ning neil olevad sertifikaadid 3 aastat, sertifikaatide lõppemisel sai sertifikaate tasuta uuendada. Alates 2007. aastast väljastatud ID-kaardid ja nende sertifikaadid kehtivad 5 aastat [30]. ID-kaardi kujunduses tehti muudatusi alles 2007. aastal [31].

2017. aasta augustis informeeriti Riigi Infosüsteemide Ametit, et on avastatud turvarisk, mis mõjutab alates 2014. aasta oktoobrist välja antud kaarte, mida oli kokku ligikaudu 750 000 [32]. Turvarisk tekkis kiibi ja tarkvara koosmõjus, kuna kiipi polnud võimalik muuta, pidid kasutajad turvariski vältimiseks kõik enda kaardi sertifikaate ja kiibitarkvara uuendama [33]. 1. aprilliks uuendati 494 000 dokumendi sertifikaadid ning ligi 300 000 dokumendi sertifikaadid tunnistati kehtetuks [34].

2018. aasta mais teatati, et Eestis on kasutusel 12 500 turvanõuetele mittevastavat ID-kaarti, mille sertifikaadid tunnistatakse kehtetuks 1. juunil. Kokku oli selliseid kaarte üle 74 000, nendest enamus on praeguseks ajaks kehtetud. Turvanõuetele ei vasta need kaardid, mis on välja antud enne 2014. aasta oktoobrit ning mida on uuendatud Politsei- ja Piirivalveameti teenindustes kaarditootja rakendusega 2012. aasta juulist kuni 2017. aasta juulini. Turvarisk seisneb selles, et osadel kaartidel genereeriti privaatvõtmed väljaspool kiipi. Riik vahetab garantiikorras välja kõik ID-kaardid, mille kehtivusaeg on pikem kui kolm kuud alates taotluse esitamisest [35].

3.2 Mobiil-ID

Mobiil-ID on elektrooniline isikutuvastusvahend, mida saab kasutada elektrooniliseks isikutuvastamiseks ja digitaalseks allkirjastamiseks mobiiltelefoni abil, sobivad nii nutitelefonid kui ka kõnetelefonid [22]. Mobiiltelefoni valiku puhul on oluline, et telefon toetaks “Sim Toolkit” nimelist tehnoloogiat [3]. Mobiil-ID-d saab kasutada kõikjal, nii Eestis kui ka välismaal, kus on mobiililevi [36].

Selleks, et Mobiil-ID-d saada, on vaja Mobiil-ID toega SIM-kaarti, selle saamiseks ja Mobiil-ID lepingu sõlmimiseks tuleb pöörduda enda mobiilioperaatori poole. Peale Mobiil-ID toega SIM-kaardi saamist tuleb Mobiil-ID kasutamiseks aktiveerida see Politsei- ja Piirivalveameti kodulehel [37].

Erinevalt teistest elektroonilistest isikut tõendavatest dokumentidest ei hoita Mobiil-ID sertifikaate SIM-kaardi kiibil [22]. Andmevahetus seadme ja e-teenuse vahel toimub üle krüpteeritud ühenduse [36].

Mobiil-ID sertifikaatide kehtivusajaks on 5 aastat. Sertifikaatide uuendamine ei ole võimalik, sertifikaatide aegumisel on vajalik uus SIM-kaart. Ühel isikul võib olla samaaegselt aktiveeritud vaid üks Mobiil-ID SIM-kaardiga seotud sertifikaadipaar [38].

Mobiil-ID elektrooniliseks kasutamiseks on vajalikud koodid: PIN1-kood on isikutuvastuseks, PIN2-kood on digitaalseks allkirja andmiseks ning PUK-kood on lukustunud PIN-koodide avamiseks [39].

E-teenusele või mobiilirakendusele Mobiil-ID liidestuse saamiseks tuleb liituda DigiDocService teenusega. See teenus võimaldab elektroonset isikutuvastust, digitaalset allkirjastamist, sertifikaatide kehtivuse kontrolli, digitaalset allkirjastamist kiipkaardiga, DigiDoc failide moodustamist ja digitaalselt allkirjastatud failide sisu ja allkirjade kehtivuse kontrolli [40].

Mobiil-ID sai alguse Eestis 2007. aastal, kui EMT koos Sertifitseerimiskeskusega tõi teenuse turule. Mobiil-ID oli suur samm edasi, kuna selle teenusega oli Eesti maailmas esimeste seas. Uudse teenuse kasutamiseks tuli kliendil sõlmida EMT-s või Elionis leping ning vahetada välja SIM-kaart [41].

2009. aasta novembrist alustas ka mobiilioperaator Elisa enda klientidele Mobiil-ID teenuse pakkumisega [42]. 2009. aasta detsembrist said ka Tele2 kliendid kasutada Mobiil-ID-d [43].

3.3 Smart-ID

Smart-ID on elektrooniline isikutuvastusvahend. Smart-ID puhul on autentimis- ja allkirjastamisvahendiks kasutaja nutiseade. Smart-ID-d saab kasutada elektrooniliseks isikutuvastuseks ning ka digitaalse allkirja andmiseks, mis küll ei ole võrdne omakäelise allkirjaga. Smart-ID loomisel on silmas peetud ka rahvusvahelist kasutust, mis tähendab, et ühes riigis tehtud Smart-ID on kasutatav ka mujal Smart-ID lahendust kasutavas riigis. Smart-ID lahendused on hetkel kasutatavad Eestis, Lätis ja Leedus [44].

Smart-ID kasutamiseks tuleb alla laadida Smart-ID *app* ning teha endale konto. Rakendus toimib iOS ja Android operatsioonisüsteemidel. Peale selle saab seda kasutada ka mitmel nutiseadmel, kasutaja peab lihtsalt registreerima eraldi konto erinevate seadmete jaoks [44].

Smart-ID kasutab kahte erinevat PIN-koodi: PIN1-koodi kasutatakse elektrooniliseks isikutuvastuseks ning PIN2-koodi kasutatakse digitaalseks allkirjastamiseks. Need mõlemad PIN-koodid saab kasutaja endale ise valida konto registreerimise ajal [45].

05.11.2016 tutvustas Sertifitseerimiskeskus Smart-ID-d [46]. 2017. aasta septembrini oli võimalik Smart-ID-d taotleda elektrooniliselt kas ID-kaardi või Mobiil-ID abil. Peale 2017. aasta septembrit oli võimalik Smart ID-d taotleda ka pangakontorites, kus teenindaja tuvastab kliendi isiku ning juhendab Smart-ID konto loomisel [47].

2018. aasta märtsi seisuga kasutab Smart-ID Baltikumis üle 750 000 kasutaja, kellest Eestis on 180 000, Lätis 330 000 ja Leedus 240 000 kasutajat [48].

3.4 Digi-ID

Digi-ID on digitaalne dokument, millega saab elektroonilises keskkonnas oma isikut tuvastada, anda digitaalset allkirja ning krüpteerida andmeid [49].

Digi-ID-d on saadaval kahte tüüpi, ühte on võimalik taotleda Eesti kodanikul, kellel on kehtiv ID-kaart ning välismaalasel, kellel on kehtiv elamisloakaart või ID-kaart [49]. Teist sorti on e-residentide Digi-ID. E-residendi Digi-ID-d võib taotleda isik, kellel on põhjendatud huvi kasutada Eesti riigi e-teenuseid [50].

Digi-ID ei ole mõeldud kasutamiseks visuaalse isikut tõendava dokumendina, seetõttu ei kanta sellele fotot, kantakse ainult nimi, isikukood, dokumendi number ning kehtivusaja lõpp [22].

Digi-ID-d saab taotleda Politsei- ja Piirivalveameti teenindustes ning see väljastatakse kohapeal ootetööna. E-residendi Digi-ID-d on võimalik taotleda e-teeninduses ning see väljastatakse taotlejale teeninduses või Eesti Vabariigi välisesinduses [50].

Digi-ID ning selle sertifikaatide kehtivusaeg on kolm aastat. Seda võib kasutada ID-kaardi kõrval paralleelselt ning selle jaoks ei ole vaja eraldi tarkvara, kuna see töötab sama tarkvaraga millega ID-kaart [49].

Digi-ID loodi 2010. aasta oktoobris ning alates 2014. aasta detsembrist saavad Digi-ID-d kasutada ka e-residendid [51].

Alates 1.05.2018 kehtib Digi-ID kolme aasta asemel viis aastat. Digi-ID kehtivust saab kauguuendamise teel pikendada alates 1. novembrist [52].

4 eID kasutusalad

Selles peatükis antakse ülevaade elektroonilise identiteedi kasutusaladest, milleks on Eestis elektrooniline isikutuvastus, digitaalne allkiri, isikule krüpteeritud andmete edastamine ja vastuvõtmine, kliendikaart ning elektrooniline võti läbipääsusüsteemides.

4.1 Elektrooniline isikutuvastus (autentimine veebikeskkondades)

Elektroonilise isikutuvastuse funktsioon võimaldab kasutajatel end interneti vahendusel turvaliselt tuvastada. See annab teenuseosutajale võimaluse veenduda, et inimene, kes kasutab antud teenust, on tõesti see inimene, kes ta väidab end olevat. Elektroonilist isikutuvastust on võimalik kasutada nii erasektori kui ka avaliku sektori veebiteenustes. See on mugav, kuna elektroonilise isikutuvastuse abil e-teenuseid kasutades jäävad paroolid samaks, seega ei pea kasutajad iga e-teenuse juures kasutama erinevat kasutajanime ja parooli ning lisaks on elektrooniline isikutuvastus palju turvalisem [53].

Selleks, et kasutajad saaksid elektrooniliselt enda isikut tuvastada, on eID vahenditel isikutuvastussertifikaat, mis sisaldab informatsiooni eID vahendi omaniku kohta. Elektrooniliseks isikutuvastuseks peab eID vahendi omanik sisestama PIN1, et tõestada teenuseosutajale, et sertifikaadil sisalduv informatsioon käib tema kohta [54].

Elektroonilise isikutuvastuse juures kasutatakse kehtivuskinnituse teenust ehk OCSP teenust, mis võimaldab küsida eID vahendite sertifikaatide kehtivuse kohta. OCSP positiivne vastus tähendab, et sertifikaat on välja antud ning on hetkel kehtiv [55]. Kehtivuskinnitusteenus sobib kõikidele e-teenustele, kus saab kasutada eID vahendit. Väljastatud sertifikaatide kehtivuskinnitusi hoitakse turvalises andmebaasis, kust on võimalik neid tõestamiseks kontrollida [56].

2016. aastal jõustus Euroopa Liidu määrus eIDAS, mille eesmärk on kergendada piiriülest e-teenuse kasutamist. eIDAS-e põhimõtteks on anda Euroopa avalikele asutustele ühtne toimimisalus elektroonilise identiteedi ja digitaalsete allkirjade tunnustamiseks. Elektroonilise isikutuvastamise tunnustamise osas on liikmesriikidel rakendamiseks aega kuni 2018. aasta sügiseni [57].

21.03.2018 seisuga on tehtud 656 510 232 elektroonilist isikutuvastust [58].

4.2 Digitaalne allkiri

Digitaalne allkiri on andmete kogum, millega allkirja andja märgib enda seost dokumendiga. Digitaalsel allkirjal on samad õiguslikud tagajärjed nagu omakäelisel allkirjal [12].

Oluline on, et digitaalsel allkirjastamisel oleks hetkel kehtiv sertifikaat, kuna ainult need allkirjad kehtivad. Sertifikaadi kehtivust kontrollitakse kehtivuskinnitusteenuse abil [59]. Kehtivuskinnitusteenus lisab digitaalsele allkirjale automaatselt elektroonilise märke, mis määrab allkirja andmise aja ja näitab, et allkirja andmise sertifikaat sel hetkel kehtis [56].

Algselt kasutati Eestis põhiliselt üht digitaalse allkirja vormingut – DDOC, millest on olemas mitmeid versioone [11]. Eesti alustas üleminekut BDOC-le 2013. aasta lõpus [60]. Uus BDOC allkirjaformaat loodi, et vahetada välja seni kasutuses olnud DDOC. BDOC formaat võeti kasutusele, kuna see on turvalisem, dokumendid on pikaajalisemalt säilivad ning paremini ühilduvad rahvusvahelises kontekstis [4].

2016. aasta veebruaris kaotati klientrakenduses DDOC-vormingus digitaalse allkirja andmise võimalus ning ainsaks formaadiks jäi BDOC ning selle alamformaat ASiC-E. ASiC-E on BDOCi rahvusvaheliseks kasutamiseks mõeldud alamformaat [61].

2017. aastal loodi tembeldamisrakendus TeRa, mis võimaldab üle tembeldada varasemalt digitaalselt allkirjastatud .ddoc formaadis olevad dokumendid. Rakenduse eesmärk on vältida dokumentide võltsimise võimalust. Kõik varasemalt antud .ddoc formaadis allkirjad jäävad kehtima, kuid pole nii muukimiskindlad. Dokumentide ületembeldamiseks tuleb rakendus käima panna ning see otsib ise arvutist ülesse kõik .ddoc formaadis olevad digitaalselt allkirjastatud dokumendid ning tõstab need koos ajatempliga uude ASiC-E konteinerisse [62].

Alates 1. juulist 2016 on kohustuslik avaliku sektori asutustel tunnustada kõikide Euroopa Liidu riikide e-allkirju vastavalt Euroopa Liidu määrusele eIDAS. Eestis saab kasutada selleks Euroopa Liidus tunnustatud .asice formaadis digitaalseid allkirju [63].

24. märtsi seisuga on antud digitaalseid allkirju 480 900 939 [58].

4.3 Isikule krüpteeritud andmete edastamine ja vastuvõtmine

Krüpteerimine on mõeldud failide turvaliseks transpordiks ebaturvalises keskkonnas. Krüpteerimine ja dekrüpteerimine toimub, kasutades autentimissertifikaati. Krüpteerimine ei ole aga mõeldud andmete pikaajaliseks säilitamiseks. Põhjuseid on mitmeid, näiteks ei ole võimalik aegunud või uuendatud sertifikaatidega enam eelmise ID-kaardi või Digi-ID sertifikaadiga krüpteeritud dokumenti dekrüpteerida. ID-kaardiga krüpteeritud dokumenti ei ole võimalik isegi samal isikul dekrüpteerida enda Digi-ID-ga [54].

Ühele krüpteeritud failile on võimalik lisada mitu dekrüpteerijat, selleks lisatakse CDOC faili kõikide vastuvõtjate sertifikaadid ja iga vastuvõtja jaoks transpordivõti dekrüpteerimiseks [6].

Dokumentide krüpteerimiseks on võimalik kasutada sümmeetrilist või asümmeetrilist krüptoalgoritmi, mis on matemaatiline valem andmefaili šifreerimiseks. Dešifreerimine on võimalik ainult krüptovõtmega. Sümmeetrilisel krüpteerimisel kasutatakse šifreerimiseks ja dešifreerimiseks ühtsama salajast võtit. Asümmeetrilisel krüpteerimisel kasutatakse šifreerimisel üht ning dešifreerimisel teist võtit, millest üks on avalik ja teine salajane kasutaja ainuomanduses asuv võti [64].

Krüpteeritud DigiDoc vormingus failide eristamiseks kasutatakse .cdoc laiendit. CDOC fail sisaldab krüpteeritud kujul andmefaili, vastuvõtja sertifikaati, krüpteeritud kujul võtit andmefaili dekrüpteerimiseks ja muid mittekohustuslikke meta-andmeid [6].

4.4 Kliendikaart

ID-kaarti ja Digi-ID-d saab kasutada ka erinevates ettevõtetes kliendikaardina. ID-kaardi ja Digi-ID kasutamine kliendikaardina on klientidele palju mugavam, kuna ID-kaart või Digi-ID on kliendil enamasti kaasas. Ka ettevõtja jaoks on ID-kaardi ja Digi-ID kasutamine kliendikaardina efektiivsem, kuna jäävad ära magnetkaartidega seotud toimingud, näiteks kaartide tellimine. Lisaks eeltoodule puudub siis ka vajadus täita ankeete, mille peavad töötajad hiljem arvutisse sisestama. ID-kaardilt ja Digi-ID-lt saavad ettevõtted lugeda välja elektrooniliselt isikuandmete faili, milles sisalduvast infost piisab

enamikele ettevõtetele [65]. ID-kaardil ja Digi-ID-l paiknev isikuandmete fail on samasugune [49].

ID-kaardi ja Digi-ID põhiseks kliendikaardisüsteemiks on müügikohas vaja ID-kaardi lugejat või ID-kaardi lugemise funktsionaalsusega kaardimakse terminali ning kassatarkvara, millel on olemas liides ID-kaardi ja Digi-ID kasutamiseks [66].

2005. aastal võttis Apollo Raamatud AS esimesena ID-kaardi enda firma kliendikaardina kasutusele [67].

4.5 Elektrooniline võti läbipääsusüsteemides

Tüüpiliselt töötavad sissepääsusüsteemid kontaktivabade kiipkaartidega. ID-kaardi ja Digi-ID kasutamine sissepääsusüsteemides on kallim ja lõppkasutajale ebamugavam kui kontaktivaba kiipkaart, kuna kasutaja peab ID-kaardi ja Digi-ID panema kaardilugejasse. Siiski on ID-kaardi ja Digi-ID kasutuselevõtt hea siis, kui kasutajate arv on väga suur ja sageli muutuv, kuna siis ei pea igale kasutajale eraldi kontaktkaarti välja andma. ID-kaardi ja Digi-ID kasutamine sissepääsusüsteemis tagab turvalisuse, kuna ID-kaarte ja Digi-ID-d on keeruline kopeerida ja neid ei anta kergekäeliselt teistele isikutele kasutamiseks [68].

ID-kaardi ja Digi-ID kasutamiseks läbipääsusüsteemides tuleb kasutajal panna ID-kaart või Digi-ID lugejasse, kust lugeja loeb välja kaardilt unikaalse teksti, registreerib selle kesksüsteemis ning kui kasutajal on selleks õigus, siis avab ukse. Kasutusel olevates süsteemides ei küsita PIN koodi [68].

Siiski on ID-kaardi ja Digi-ID kasutamisel ka omad miinused. ID-kaart ja Digi-ID ei ole väga kulumiskindel, seetõttu ei ole see sobilik kohtades, kus on vaja seda palju kasutada. Peale selle ei ole võimalik süsteemi kasutada inimestel, kellel puudub ID-kaart või Digi-ID, näiteks välismaalastel kellel ei ole võimalik ID-kaarti teha või kelle jaoks Digi-ID tegemine on liiga kulukas. Kui kasutajal peaks ID-kaart või Digi-ID kaduma, siis pole tal võimalik ligi pääseda nii kaua, kuni ta uue kaardi saab [68].

4.6 Kasutusalad erinevate eID vahenditega

Erinevaid eID vahendeid on võimalik kasutada erinevateks kasutusaladeks. Kõikide eID vahenditega ei ole võimalik kasutada kõiki töös kirjeldatud kasutusalasid.

Alljärgnevas tabelis tuuakse välja, milliseid eelnevalt kirjeldatud kasutusalasid on võimalik töös kirjeldatud Eesti elektroonilise identiteedi vahenditega kasutada.

Tabel 1. Erinevate eID vahendite kasutusalad.

	Elektrooniline isikutuvastus	**Digitaalne allkiri**	**Krüpteerimine**	**Kliendikaart**	**Läbipääsusüsteemid**
ID-kaart	x	x	x	x	x
Digi-ID	x	x	x	x**	x**
Mobiil-ID	x	x			
Smart-ID	x	x*			

** Smart-ID-ga antud allkiri ei ole võrdne omakäelise allkirjaga* [69].
*** Digi-ID-d saab kasutada lisaks ID-kaardile kliendikaardina ja läbipääsusüsteemides, kuna Digi-ID-l ja ID-kaardil on samasugune isikuandmetefail* [49].

5 eID välismaal

Selles peatükis antakse ülevaade mõningatest eID vahenditest erinevates riikides. Antud peatükis ei tooda välja ülevaadet eID kasutusalade kohta, kuna välismaal puuduvad uudsed lahendused kasutusaladeks. Välismaal kasutatakse eID-d elektrooniliseks isikutuvastuseks ning digitaalseks allkirjastamiseks või ainult elektrooniliseks isikutuvastuseks. Elektrooniliseks isikutuvastuseks ja digitaalseks allkirjastamiseks saab eID vahendit kasutada näiteks Belgias, Itaalias, Portugalis, Hispaanias. Panga poolt väljastatud eID vahendit saab kasutada elektrooniliseks isikutuvastuseks näiteks Norras, Rootsis ja Soomes [70].

5.1 DigiD

DigiD on Hollandis kasutusel olev eID vahend, millega pääsevad hollandlased ligi valitsuse veebilehtedele, näiteks Hollandi maksuameti, politsei, tervishoiuteenuse osutajate, seehulgas ka apteegid, pensionifondide ja paljudele teistele veebilehekülgedele [71]. DigiD koosneb kasutajanimest ja paroolist, mille kasutaja saab endale ise valida. Kasutajanimele ja paroolile saab juurde lisada ka täiendava kinnituse SMS-i teel, see on soovitatav, kuna osadel veebilehtedel on nõutav selline täiendav kinnitus [72]. DigiD ei ole kohustuslik, kuid ilma selleta ei ole võimalik valitsuse veebilehtedele ligi pääseda [73].

DigiD saamiseks peab kasutaja esitama taotluse DigiD veebilehel, seejärel saab kasutaja SMS koodi, mille ta peab sisestama veebileheküljel ning siis peab ta sisestama uue koodi, mille saab e-posti teel. Peale seda saadetakse kasutajale posti teel aktiveerimiskood, millega ta peab enda DigiD aktiveerima 20 päeva jooksul [71]. DigiD saavad taotleda ja kasutada ka välismaal elavad hollandlased. Taotluse esitamine käib sarnaselt, kuid aktiveerimiskoodi saamiseks peavad välismaal elavad hollandlased 30 päeva jooksul pöörduma DigiD väljastavasse esindusse, milleks on kas Hollandi linnavalitsused või Hollandi saatkonnad [74].

DigiD-ga sisse logimiseks peab kasutaja minema veebilehele, kuhu ta soovib sisse logida. Seejärel suunatakse kasutaja DigiD sisselogimislehele, kuhu kasutaja sisestab enda DigiD

kasutajanime ja parooli ning seejärel suunatakse ta tagasi veebilehele, kuhu ta soovis sisse logida [72].

5.2 Norra 5 elektroonilist ID-d

Norra riigiasutuste elektrooniliste teenuste kasutamiseks peab norralasel olema elektrooniline ID. Elektrooniliste teenuste kasutamiseks, saavad norralased valida viie erineva elektroonilise ID vahel, milleks on: MinID, BankID, BankID mobiiltelefonis, Buypass või Commfides [75].

Teenuse omanik määrab, millist turvalisuse taset tema teenus vajab, kas keskmise turvalisuse tasemega või kõrgeima turvalisuse tasemega. Turvalisuse taseme valik sõltub sellest, millist teenust pakutakse ning millised võivad tagajärjed olla õnnetuse korral. Min-ID kasutab keskmist turvalisuse taset 3. BankID, BankID mobiilile, Buypass ja Commfides kasutavad kõrgeimat turvalisuse taset 4. Min-ID turvalisuse tagab kahefaktoriline autentimine, mis koosneb isikukoodist, paroolist ning midagi mis on ainult kasutajal ehk koodid. Turvalisuse tase 4 kasutab ka kahefaktorilist autentimist, kuid eID antakse kasutajale silmast-silma kohtumisel, kus tehakse kindlaks isik, vältimaks isiku eID sattumist valdesse kätesse [76].

MinID on isiklik elektrooniline ID, mille kasutamiseks peab kasutaja olema vähemalt 13 aastane. MinID saamiseks on vaja riikliku identifitseerimisnumbrit, mobiilinumbrit või e-posti aadressi ja PIN-koode [75]. PIN-koodid saadetakse aadressile, mille on kasutaja registreerinud Norra rahvusregistris [77].

BankID on isiklik elektrooniline ID, mille saamiseks peab ühendust võtma enda pangaga. BankID saamiseks peab olema vähemalt 15 aastane [75].

BankID mobiiltelefonile on elektrooniline ID, mille saamiseks peab ühendust võtma enda pangaga. BankID saamiseks mobiiltelefonile peab olemas olema BankID koodid [75].

Buypass ID on isiklik elektrooniline ID, selle väljastab Buypass AS, Buypassi ID-d on võimalik kasutada kiipkaardil või Buypass ID-d mobiilis. Buypassil ei ole vanuse piirangut [75]. Buypass kiipkaardid on saadaval erinevates kujundustes. Kaardid antakse välja koos kvalifitseeritud elektroonilise ID-ga koos PKI-ga [78]. Buypassi kiipkaardi kasutamiseks on vaja panna kaart kaardilugejasse ja sisestada PIN-kood [79].

Commfiedes on isiklik elektrooniline ID, mis on pandud turvaliselt USB pulgale. Sellel ei ole vanuse piirangut, kuid see vajab isiklikku allkirja [75].

5.3 NemID

NemID on Taanis kasutusel olev kokkuvolditud paber, millel on koodid. Kokkuvolditud paberit saab kasutada turvaliselt veebilehtedele sisse logimiseks [80]. NemID koosneb kasutajanimest, paroolist ning koodikaardist, millel on ühekordsed koodid. Sisselogimiseks tuleb esmalt sisestada kasutajanimi ja parool ning seejärel kood koodikaardilt [81].

NemID saamiseks peab olema vähemalt 15-aastane ja omama isikukoodi. NemID saavad omada ka isikud, kes ei ole taanlased, kui on olemas Taani elamisluba või kasutaja õpib Taanis [82].

5.4 DNIe

DNIe ehk Documento Nacional de Identidad electrónico on Hispaanias eID vahendina kasutusel. See on kooskõlas EL direktiiviga, mis käsitleb elektroonilist ID-d. DNIe on kiipkaart, millel on sertifikaadid elektrooniliseks isikutuvastuseks ning digitaalseks allkirjastamiseks. See on sarnane Eesti ID-kaardile [83].

Kaarte antakse Hispaania kodanikele ning seda saab kasutada ka lihtsalt dokumendina isiku tuvastamiseks. Selleks, et seda elektrooniliselt kasutada, peab kasutaja minema politseijaoskonda ning aktiveerima kiibi [83].

6 Töös kasutatavate analüüsimetoodikate kirjeldus

Selles peatükis antakse ülevaade lõputöös kasutatavatest analüüsimetoodikatest, milleks on SWOT – analüüs, riskianalüüs ja internetiküsitlus.

6.1 SWOT – analüüs

Elektroonilise identiteedi vahendite analüüsiks saab kasutada rahvusvaheliselt tuntud SWOT analüüsimeetodit. See meetod võimaldab saada põhjaliku ülevaate elektroonilise identiteedi vahendite tugevatest ja nõrkadest külgedest ning väliskeskkonnast tulenevatest ohtudest ja võimalustest.

SWOT - analüüsi nimi tuleneb inglise keelsetest sõnadest: S - *strengths* (tugevused), W - *weaknesses* (nõrkused), O - *opportunities* (võimalused), T - *threats* (ohud) [84].

SWOT - analüüsi eeliseks on, et sellega on võimalik kiiresti hinnata eID vahendi seisundit. Positiivne SWOT - analüüsi juures on, et see annab hea ülevaate ning on laialdaselt levinud ja selle kohta on palju abistavat informatsiooni saadaval.

Negatiivsetest külgedest võib välja tuua selle, et SWOT - analüüsi võidakse kasutada valesti, kuna tabelit täidetakse valesti ja täitmisel ei olda ausad ning töö lõpetatakse enne, kui see tegelikult valmis on. Seetõttu võib selle meetodi kasutegur olla väike [85].

6.2 Riskianalüüs

Riskide hindamisel tuleb esmalt kaardistada, millised riskid võivad ohustada eID vahendeid. Riskide kaardistamisel kasutatakse SWOT - analüüsi käigus selgunud väliskeskkonnast tulenevaid ohtusid. Kui riskid on kaardistatud, siis tuleb läbi viia riskide hindamine, see tähendab, et iga kaardistatud riski juures hinnatakse tema esinemise tõenäosust ning sellega kaasnevat mõju. Hindamise skaalal kasutatakse 4-punktist skaalat (vt. Tabel 1.) [86].

Tabel 2. Riskide hindamise 4-punktiline skaala [86].

Hinne	**Hinnang**	**Mõju**	**Hinnang**	**Tõenäosus**
1	Tähtsusetu mõju	Riski avaldumine ei häiri planeeritavaid tegevusi ning eesmärkide saavutamist.	Vähetõenäoline	Riski avaldumine on pigem teoreetiline, praktikas üliharvad juhtumid.
2	Vähene mõju	Riski avaldumisel on tegevused ja eesmärkide saavutamine mõningal määral häiritud, kuid eesmärgid on saavutatavad.	Võimalik	Riski avaldumine on võimalik aga praktilisi juhtumeid on üksikuid.
3	Oluline mõju	Riski avaldumisel on tegevused ja eesmärkide saavutamine oluliselt häiritud.	Tõenäoline	Riski avaldumine on suure tõenäosusega ning on olemas kindlad tõendusmaterjalid riski avaldumise kohta.
4	Kahjustav mõju	Riski avaldumisel ei ole võimalik tegevusi jätkata ja/või eesmärke saavutada.	Kindel	Risk on juba avaldunud või riski avaldumine tulevikus on vältimatu.

6.3 Internetiküsitlus

Internetiküsitlus on kiiresti populaarsust koguv võimalus küsitluste läbiviimiseks, kuna interneti kasutajate arv kasvab kiiresti. Internetiküsitlusel tuleb arvesse võtta uuritav sihtrühm, kuidas leida vastajaid, kui palju küsimusi esitada ning kuidas tulemusi hinnata [87].

Internetiküsitluste tehniline koostamine on tänapäeval väga kergeks tehtud. Selleks on loodud erinevaid küsitluse koostamise veebilehekülgi, mida on väga mugav kasutada. Koostamiseks on saadaval näiteks Google Forms, Formstack, Wofoo, Typeform ja palju teisi [88].

Internetiküsitluse eelisteks on küsitluse täitmise kiirus ja mugavus, kuna vastajad saavad seda teha neile sobival ajal sobivas kohas, lisaks saavad vastajad rahulikult mõelda küsimuse üle ja oma mõtted korralikult kirja panna. Lisaks on hea ja mugav ka jooksvalt tulemusi jälgida ning tulemuse kokkuvõtte tegemine on kiirem.

Internetiküsitluse miinusteks on piiratud kasutajaskond, kuna on raske jõuda inimesteni kellel ei ole kodus arvutit või internetiühendust, ning ka nendeni, kes kasutavad arvutit või internetti harvem. Üheks probleemiks on ka see, et on raske leida õiget kanalit, mille kaudu edastada küsimustikku enda sihtrühmale. Samuti puudub internetiküsitluse juures võimalus esitada täpsustavaid küsimusi.

7 eID vahendite analüüs

Selles peatükis rakendatakse Eesti eID vahendite ja nende kasutusalade analüüsiks eelmises peatükis kirjeldatud SWOT – analüüsi, riskianalüüsi ja internetiküsitlust.

7.1 SWOT - analüüs

Alljärgnevas tabelis esitatakse ID-kaardi tugevused, nõrkused, võimalused ja ohud.

Tabel 3. SWOT - analüüs ID-kaart.

***Strenghts*/Tugevused**	***Weaknesses*/Nõrkused**
▪ ID-kaart on isikut tõendava dokumendina kohustuslik ning lisaväärtusena on võimalik seda kasutada ka digitaalselt [23]. ▪ PIN ja PUK koodide unustamisel, kaotamisel või PUK koodi lukustamisel on võimalik uued koodid saada kas Politsei- ja Piirivalveameti teenindusest või pangakontorist. Koodid väljastatakse kohapeal koheselt [89]. ▪ Pikalt turul olnud. ▪ Põhjalikud juhendid id.ee lehel eesti, vene ja inglise keeles.	▪ Suured kulud kriiside lahendamisel [90]. ▪ Uue ID-kaardi saamisel või sertifikaatide uuendamisel ei ole võimalik vanade sertifikaatidega või dokumendiga krüpteeritud faile dekrüpteerida [91]. ▪ Vajab elektrooniliseks kasutamiseks kaardilugejat, ID-kaardi tarkvara ja kehtivaid sertifikaate [27]. ▪ Kehtivusaeg on 5 aastat ning peale seda tuleb taotleda uus ID-kaart [23]. ▪ ID-kaardi väljastamine võib võtta aega kuni 30 päeva, dokumendi kaotamisel ei ole võimalik ID-kaarti kasutada selle perioodi jooksul [92]. ▪ ID-kaarti väljastatakse ainult Politsei- ja Piirivalveameti teenindustes või Eesti Vabariigi välisesindustes, kus on võimalik dokumendile järgi minna piiratud ajal ja piiratud asukohtades [93].
***Opportunities*/Võimalused**	***Threats*/Ohud**
▪ Palju kasutusalasid, võimaldab lisaks elektroonilisele isikutuvastusele ja digitaalsele allkirjastamisele dokumentide krüpteerimist, kliendikaardina ning ligipääsusüsteemides kasutamist. ▪ Riigipoolne tugi.	▪ Veebitarkvara areneb kiirelt ja pidevalt ning uute turvanõuetega võib kaduda ID-kaardi tugi mõnelt veebilehitsejalt enne, kui on jõutud ID-kaardi tarkvarale leida täiendus [3]. ▪ Tarkvara on kasutajatele keeruline, seetõttu võivad kasutajad valida muu elektroonilise identiteedi vahendi [3]. ▪ ID-kaardi tarkvaras on toetatud kindlad operatsioonisüsteemid, seetõttu võib tugi

▪ Taotlust uue ID-kaardi saamiseks on võimalik esitada ka Politsei- ja Piirivalveameti e-teeninduses [23]. ▪ Vajalik teiste vahendite juures isikustamiseks.	puududa vananenud, vähese kasutusega või uudsetel operatsioonisüsteemidel [94]. ▪ Küberrünnakud.

Alljärgnevas tabelis esitatakse Mobiil-ID tugevused, nõrkused, võimalused ja ohud.

Tabel 4. SWOT - analüüs Mobiil-ID.

***Strenghts*/Tugevused**	***Weaknesses*/Nõrkused**
▪ Kasutamiseks sobivad nii nutitelefonid kui ka kõnetelefonid [36]. ▪ Saab kasutada igal pool maailmas, kus on mobiililevi [36]. ▪ Telefoni kaotamisel on võimalik mobiilioperaatoril SIM-kaart lukustada ning Mobiil-ID kasutamine peatada [39]. ▪ Kasutamiseks ei ole vaja kaardilugejat või spetsiaalset tarkvara [39].	▪ Mobiil-ID saamiseks tuleb SIM-kaart välja vahetada [95]. ▪ Mobiil-ID lepingu sõlmimiseks tuleb pöörduda mobiilioperaatori poole ning aktiveerida teenus [95]. ▪ Ühele isikule saab vormistada ainult ühe Mobiil-ID lepingu [95]. ▪ PIN ja PUK koodide unustamisel või PUK-koodi lukustamisel on tarvis uut SIM-kaarti [96]. ▪ Mobiil-ID sertifikaatide aegumisel tuleb teha uus SIM-kaart [38]. ▪ Mobiil-ID saamiseks peab olema vähemalt 15 aastane [95]. ▪ Mobiil-ID-d ei saa kasutada kasutajad, kellel ei ole mõnda muud eID vahendit, kuna Mobiil-ID teenuse aktiveerimiseks Politsei- ja Piirivalveameti e-teeninduses on vaja mõnda muud eID vahendit [97].
***Opportunities*/Võimalused**	***Threats*/Ohud**
▪ Mobiil-ID tugi on paljudel Eesti e-teenustel ja mobiilirakendustel [39]. ▪ Digitaalne allkiri on võrdne omakäelise allkirjaga [39]. ▪ Mobiil-ID on riiklikult tunnustatud [98].	▪ Kasutajad ei vali Mobiil-ID-d suure tasu tõttu. Iga Mobiil-ID kasutaja peab iga kuu maksma Elisas ja Telias 1 euro ning Tele2-s 0,99 eurot, mis teeb 5 aasta jooksul 60 eurot [95]. ▪ Mobiil-ID kasutamine välismaal võib tuua kasutajatele suure telefoniarve, kuna välismaal Mobiil-ID kasutamisel lisandub välisriigist Eestisse saatmise SMS-i hind ühe toimingu kohta [95].

Alljärgnevas tabelis esitatakse Digi-ID tugevused, nõrkused, võimalused ja ohud.

Tabel 5. SWOT - analüüs Digi-ID.

***Strenghts*/Tugevused**	***Weaknesses*/Nõrkused**
▪ PIN ja PUK koodide unustamisel, kaotamisel või PUK koodi lukustamisel on võimalik uued koodid saada kas Politsei- ja Piirivalveameti teenindusest või pangakontorist, mis väljastatakse kohapeal koheselt [49]. ▪ Ei ole vaja eraldi tarkvara, töötab sama tarkvaraga millega ID-kaart [49]. ▪ Digi-ID-d on võimalik kasutada lisaks elektroonilisele isikutuvastusele ja digitaalsele allkirjastamisele ka dokumentide krüpteerimiseks, kliendikaardina ning läbipääsusüsteemides [49].	▪ Digi-ID ei ole mõeldud kasutamiseks visuaalse isikut tõendava dokumendina [22]. ▪ Digi-ID kehtivusaeg on 3 aastat [49]. ▪ E-residendil on raske abi saada kui ta paikneb välismaal, kuna Politsei ja Piirivalveameti teeninduse poole pöördumise võimalus puudub.
***Opportunities*/Võimalused**	***Threats*/Ohud**
▪ Digi-ID valmistatakse Politsei- ja Piirivalveametis teeninduses kohapeal ootetööna [92]. ▪ Saavad kasutada ka välismaalased, kellel on huvi kasutada Eesti riigi e-teenuseid [50]. ▪ Riigipoolne tugi. ▪ Alates 1.05.2018 kehtib Digi-ID kolme aasta asemel viis aastat [52].	▪ Veebitarkvara areneb kiirelt ja pidevalt ning uute turvanõuetega võib kaduda Digi-ID tugi mõnelt veebibrauserilt enne kui on jõutud tarkvarale leida täiendus [3]. ▪ E-residendid ei vali Digi-ID-d või ei taotle uut e-residendi Digi-ID-d suure riigilõivu tõttu, milleks on 100 eurot [50]. ▪ ID-kaardi tarkvaras on toetatud kindlad operatsioonisüsteemid, seetõttu võib tugi puududa vananenud, vähese kasutusega või uudsetest operatsioonisüsteemidest [94]. ▪ Küberrünnakud.

Alljärgnevas tabelis esitatakse Smart-ID tugevused, nõrkused, võimalused ja ohud.

Tabel 6. SWOT - analüüs Smart-ID.

***Strenghts*/Tugevused**	***Weaknesses*/Nõrkused**
▪ Saab kasutada mitme nutiseadmega [44].	▪ Kolmandal korral PIN-koodide valesti sisestamisel lukustatakse konto lõplikult

▪ Kasutamiseks ei ole vaja täiendavaid lisaseadmeid nagu spetsiaalne SIM-kaart või kaardilugeja [44]. ▪ Vanuselised piirangud kasutamiseks puuduvad [99]. ▪ Nutiseadme kaotamisel või varastamisel on võimalik konto kustutada iseteenindusportaalis või klienditeenindusega ühendust võttes [100]. ▪ Smart-ID allalaadimine ning kasutamine on tasuta kasutajale [101]. ▪ Kui kontoga on liidetud mitu seadet ning keegi soovib mõnes teises seadmes sisse logida, siis kuvatakse teavitus igas seadmes, siis on teada kui keegi teine soovib kasutada sinu kontot [102]. ▪ Ühe Android seadmega on võimalik kasutada mitut erinevat Smart-ID kontot, kui nutiseade toetab mitme kasutaja profiile [100].	ning edasiseks kasutamiseks tuleb vana konto kustutada ja uus konto luua [103]. ▪ PIN-koodide unustamisel tuleb vana konto kustutada ja uus konto luua edasiseks kasutamiseks [104]. ▪ Kui konto loomisel kasutada isiku tuvastamiseks panga koodikaarte, siis saab edaspidi Smart-ID-d kasutada ainult pangateenustes [100]. ▪ PIN-koode pole võimalik muuta, ainus võimalus on konto kustutada ja uus konto luua erinevate PIN-koodidega [100]. ▪ Smart-ID-d ei saa kasutada e-hääletamiseks [105]. ▪ Smart-ID-d ei saa kasutada kasutajad, kellel ei ole mõnda muud eID vahendit, kuna Smart-ID konto aktiveerimiseks on tarvis isik tuvastada kasutades mõnda muud eID vahendit [101].
***Opportunities*/Võimalused**	***Threats*/Ohud**
▪ Ühes riigis väljastatud Smart-ID-d saab kasutada ka mujal Smart-ID lahendust kasutavas riigis [44]. ▪ Konto saab luua kodust lahkumata endale sobival ajal ja kohas. ▪ Smart-ID konto on aktiivne 3 aastat, kuid enne eelmise konto kehtivusaja lõppemist on võimalik luua juba uus konto [100].	▪ Smart-ID-d ei ole võimalik kasutada paljudel veebilehekülgedel elektrooniliseks isikutuvastuseks, kuna vähesed teenuse osutajad on liidestunud Smart-ID-ga. ▪ Smart-ID-d ei ole võimalik kasutada digitaalseks allkirjastamiseks infovahetuses riigiga, kuna Smart-ID-ga antud digitaalne allkiri ei ole võrdne omakäelise allkirjaga [69]. ▪ Smart-ID-d ei ole võimalik kasutada kõikide nutiseadmete operatsioonisüsteemidega. ▪ Smart-ID-d ei ole võimalik kasutada ilma internetiühenduseta [100]. ▪ Smart-ID-d saab kasutada vaid nutitelefoni või tahvelarvuti omanik [101].

Mobiil-ID ja Smart-ID üheks suuremaks nõrkuseks on see, et neid ei ole võimalik kasutada, kui kasutajal puudub lisaks mõni muu eID vahend, millega isikut tuvastada.

Mobiil-ID-d saab aktiveerida Politsei- ja Piirivalveameti e-teeninduses, kus on võimalik kasutada ID-kaarti, Digi-ID-d või elamisloakaarti. Smart-ID-s isiku tuvastamiseks on võimalik ka kasutada internetipanka, kuid internetipangaga isiku tuvastamisel on võimalik Smart-ID-d edaspidi kasutada vaid internetipangas. Samuti on Smart-ID ning Mobiil-ID üheks nõrkuseks ka see, et PIN ja PUK koodide kaotamisel või unustamisel ei ole võimalik saada uusi koode, vaid tuleb teha uus Smart-ID või Mobiil-ID. Smart-ID puhul on suurematekst ohtudeks see, et seda pole võimalik kasutada paljudel veebilehekülgedel kus puudub Smart-ID tugi ning Smart-ID-d ei ole võimalik kasutada digitaalseks allkirjastamiseks riiklikes teenustes, kuna Smart-ID-ga antud digitaalne allkiri ei ole võrdsustatud omakäelise allkirjaga.

ID-kaardi ja Digi-ID üheks suurimaks ohuks on see, et veebibrauseritelt võib kaduda ID-kaardi tarkvara tugi, tarkvara parandamisele võib minna palju aega, murele ei pruugita leida lahendust ning kasutajad ei pruugi saada mõnda aega enda valitud veebibrauserit kasutada. Samuti ei saa kasutada ID-kaarti ja Digi-ID-d operatsioonisüsteemides, millel puudub ID-kaardi tarkvara tugi.

Võimalusterohkeimaks eID vahendiks on ID-kaart, kuna antud eID vahendit on võimalik kasutada paljudel eesmärkidel ning ID-kaart on vajalik teiste eID vahendite juures isiku tuvastamiseks. Erinevalt Mobiil-ID-st ja Smart-ID-st on ID-kaardil ja Digi-ID-l võimalik taotleda uued koodid.

7.2 Riskianalüüs

See peatükk on jagatud 4 osaks. Osad koosnevad ID-kaardi, Mobiil-ID, Digi-ID ja Smart-ID riskidest, mis selgitati välja SWOT – analüüsi käigus.

7.2.1 ID-kaardi riskid

Risk 1: Veebitarkvara areneb kiirelt ja pidevalt ning uute turvanõuetega võib kaduda ID-kaardi tugi mõnelt veebilehitsejalt enne, kui on jõutud ID-kaardi tarkvarale leida täiendus [3].

Hinnang: 4

Mõju: Riski avaldumisel ei ole võimalik ID-kaardi tarkvara kasutada probleemses veebilehitsejas ning probleemi lahendamiseks on vaja oodata veebilehitseja tuge tehnilise võimekuse loomisel [106].

Tõenäosus: Risk on juba avaldunud mõnel korral ning riski avaldumine tulevikus on vältimatu, kuna veebilehitsejad arenevad kiirelt ja pidevalt. MacOS 10.12 Sierra kasutamisel ei olnud võimalik kasutada Safari veebilehitsejat ID-kaardiga autentimiseks ja allkirjastamiseks [107]. Samuti ei saanud peale sertifikaatide uuendamist MacOS operatsioonisüsteemi kasutajad ID-kaarti kasutada Safari ja Google Chrome veebilehitsejaga, kuna veebilehitsejad ei toetanud uut kasutusele võetavat krüptoalgorütmi [106].

Risk 2: Tarkvara on kasutajatele keeruline, seetõttu võivad kasutajad valida muu elektroonilise identiteedi vahendi [3].

Hinnang: 2

Mõju: Riski avaldumisel on võimalik, et kasutajad valivad uue vahendi, kuigi kasutajatel on võimalus küsida abi ööpäevaringselt ID-abiliinilt.

Tõenäosus: Riski avaldumine on võimalik, kuid pigem teoreetiline, kuna kasutajad, kes kasutavad elektroonilist identiteeti harva, pigem ei vali muud vahendit lisakulude või ümberharjumise raskuste tõttu.

Risk 3: ID-kaardi tarkvaras on toetatud kindlad operatsioonisüsteemid, seetõttu võib tugi puududa vananenud, vähese kasutusega või uudsetest operatsioonisüsteemidest [94].

Hinnang: 4

Mõju: Riski avaldumisel ei ole võimalik ID-kaardi tarkvara kasutada mittetoetatud operatsioonisüsteemides. Kasutajad, kes kasutavad vananenud operatsioonisüsteemi, saavad ID-kaarti kasutada, kui nad uuendavad enda arvuti operatsioonisüsteemi. Kui aga esineb probleem vähese kasutusega operatsioonisüsteemiga, millele ei ole loodud tuge, siis kasutajatel ei olegi võimalik kasutada antud operatsioonisüsteemis ID-kaardi tarkvara, näiteks vähem levinumad Linuxi distributsioonid, millel on vähe kasutajaid, nagu Linux Mint ja Fedora. Kasutajad, kes kasutavad uudset operatsioonisüsteemi, millele ei ole jõutud ID-kaardi tarkvara tuge luua, peavad ootama toe tulekuni.

Tõenäosus: Risk on juba avaldunud ning riski avaldumine tulevikus on vältimatu, kuna operatsioonisüsteemid arenevad kiirelt ning tugi vanadelt operatsioonisüsteemidelt või väheste kasutajatega operatsioonisüsteemidel puudub. Tugi on enamasti olemas paaril viimasel operatsioonisüsteemil [108].

Risk 4: Küberrünnakud.

Hinnang: 1

Mõju: Mõjutab kõiki turvanõrkusega ID-kaarte.

Tõenäosus: Riski avaldumine on pigem teoreetiline, kuna turvavõtme lahti murdmine võtab kaua aega ning on väga kulukas [109]. 2017. aasta augustis avastati ID-kaardi ja Digi-ID kiipides turvanõrkus mis puudutas ligi 750 000 kaarti [32]. 750 000 kaardist ühtegi lahti ei murtud [109].

7.2.2 Mobiil-ID riskid

Risk 1: Kasutajad ei vali Mobiil-ID-d suure tasu tõttu. Iga Mobiil-ID kasutaja peab iga kuu maksma Elisas ja Telias 1 euro ning Tele2-s 0,99 eurot, mis teeb 5 aasta jooksul 60 eurot [95].

Hinnang: 1

Mõju: Mobiil-ID kasutajate langus. Kasutajad võivad valida mõne muu elektroonilise identiteedi vahendi, kuna teised eID vahendid on oluliselt odavamad kui Mobiil-ID.

Tõenäosus: Riski avaldumine on pigem teoreetiline, kuna Mobiil-ID-l oli 2017. aasta lõpu seisuga aktiivseid kasutajaid 134 888 [110].

Risk 2: Mobiil-ID kasutamine välismaal võib tuua kasutajatele suure telefoniarve, kuna välismaal Mobiil-ID kasutamisel lisandub välisriigist Eestisse saatmise SMS-i hind ühe toimingu kohta [95].

Hinnang: 3

Mõju: Risk avaldub kõikidel välismaal paiknevatel Mobiil-ID kasutajatel.

Risk avaldub kasutajatel, kes ei ole teadlikud, et Mobiil-ID kasutamise korral saadab kliendi telefon kaks SMS-i, üks isiku tuvastamiseks ning teine digitaalse allkirja andmiseks. Seetõttu võib välismaal Mobiil-ID kasutamine tuua kaasa suure telefoniarve [111].

Tõenäosus: Risk on juba avaldunud. Ühel Mobiil-ID kasutajal tuli tavapärasest ligi 80 eurot suurem mobiiliarve, kuna kasutaja ei olnud teadlik, et Mobiil-ID kasutab SMS-de saatmist, mis lisandub tema telefoniarvele välismaal SMS-de saatmise hinnakirja põhiselt [111].

7.2.3 Digi-ID riskid

Risk 1: Veebitarkvara areneb kiirelt ja pidevalt ning uute turvanõuetega võib kaduda Digi-ID tugi mõnelt veebibrauserilt enne kui on jõutud tarkvarale leida täiendus [3].

Hinnang: 4

Mõju: Riski avaldumisel ei ole võimalik ID-kaardi tarkvara kasutada probleemses veebilehitsejas ning probleemi lahendamiseks on vaja oodata veebilehitseja arendaja tuge tehnilise võimekuse loomisel [106].

Tõenäosus: Risk on juba avaldanud mõnel korral ning riski avaldumine tulevikus on vältimatu, kuna veebilehitsejad arenevad kiirelt ja pidevalt. MacOS 10.12 Sierra kasutamisel ei olnud võimalik kasutada Safari veebilehitsejat ID-kaardiga autentimiseks ja allkirjastamiseks [107]. Samuti ei saanud peale sertifikaatide uuendamist MacOS operatsioonisüsteemi kasutajad ID-kaarti kasutada Safari ja Google Chrome veebilehitsejaga, kuna veebilehitsejad ei toetanud uut kasutuselevõetavat krüptoalgorütmi [106].

Risk 2: E-residendid ei vali Digi-ID-d või ei taotle uut e-residendi Digi-ID-d suure riigilõivu tõttu, milleks on 100 eurot.

Hinnang: 2

Mõju: E-residendi Digi-ID kasutajate vähenemine.

Tõenäosus: Riski avaldumine on pigem teoreetiline, kuna e-residendi Digi-ID on ainus võimalus välismaalasel Eestis elektroonilises keskkonnas asjade ajamiseks, olenemata tema füüsilisest asukohast.

Risk 3: ID-kaardi tarkvaras on toetatud kindlad operatsioonisüsteemid, seetõttu võib tugi puududa vananenud, vähese kasutusega või uudsetest operatsioonisüsteemidest [94].

Hinnang: 4

Mõju: Riski avaldumisel ei ole võimalik ID-kaardi tarkvara kasutada mittetoetatutes operatsioonisüsteemides. Kasutajad, kes kasutavad vananenud operatsioonisüsteemi, saavad ID-kaarti kasutada kui nad uuendavad enda arvuti operatsioonisüsteemi. Kui aga esineb probleem vähese kasutusega operatsioonisüsteemiga, millele ei ole loodud tuge, siis kasutajatel ei olegi võimalik kasutada antud operatsioonisüsteemis ID-kaardi tarkvara, näiteks Linuxi distributsioone, millel on vähe kasutajaid nagu Linux Mint ja Fedora. Kasutajad, kes kasutavad uudset operatsioonisüsteemi, millele ei ole jõutud ID-kaardi tarkvara tugi luua, peavad ootama toe tulekuni.

Tõenäosus: Risk on juba avaldunud ning riski avaldumine tulevikus on vältimatu, kuna operatsioonisüsteemid arenevad kiirelt ning tugi vanadelt operatsioonisüsteemidelt või väheste kasutajatega operatsioonisüsteemidel puudub. Tugi on enamasti olemas paaril viimasel operatsioonisüsteemil [108].

Risk 4: Küberrünnakud.

Hinnang: 1

Mõju: Mõjutab kõiki Digi-ID turvanõrkusega kaarte.

Tõenäosus: Riski avaldumine on pigem teoreetiline, kuna turvavõtme lahti murdmine võtab kaua aega ning on väga kulukas [109]. 2017. aasta augustis avastati ID-kaardi ja Digi-ID kiipides turvanõrkus mis puudutas ligi 750 000 kaarti [32]. 750 000 kaardist ühtegi lahti ei murtud [109].

7.2.4 Smart-ID riskid

Risk 1: Smart-ID-d ei ole võimalik kasutada paljudel veebilehekülgedel elektrooniliseks isikutuvastuseks, kuna vähesed teenuse osutajad on liidestunud Smart-ID-ga.

Hinnang: 4

Mõju: Smart-ID kasutajad ei saa kasutada Smart-ID-d elektrooniliseks isikutuvastuseks paljudel veebilehekülgedel. Veebilehekülje sisenemiseks peavad kasutajad valima mõne muu eID vahendi.

Tõenäosus: Riski avaldumine on vältimatu, kuna ligipääs paljudesse e-teenustesse puudub Smart-ID-ga, näiteks kõikidele riigiteenustele.

Risk 2: Smart-ID-d ei ole võimalik kasutada digitaalseks allkirjastamiseks infovahetuses riigiga, kuna Smart-ID-ga antud digitaalne allkiri ei ole võrdne omakäelise allkirjaga [69].

Hinnang: 4

Mõju: Smart-ID kasutajad ei saa kasutada Smart-ID-d digitaalseks allkirjastamiseks olukordades, kus nõutakse, et antud allkirjad oleksid võrdelised omakäelise allkirjaga. Sellistes olukordades peavad kasutajad valima mõne muu eID vahendi. Kasutajad, kes kasutavad Smart-ID-d digitaalse allkirja andmiseks kasutades näiteks veebilehekülge digidoc.ee, mis võimaldab ka digitaalset allkirja anda Smart-ID-ga erinevalt ID-kaardi tarkvarast, peavad sellised dokumendid uuesti allkirjastama mõne muu identiteedi vahendiga.

Tõenäosus: Riski avaldumine on vältimatu, kuna Smart-ID-ga antud allkiri ei ole võrdeline omakäelise allkirjaga, mis on vajalik infovahetuses riigiga.

Risk 3: Smart-ID-d ei ole võimalik kasutada kõikide nutiseadmete operatsioonisüsteemidega.

Hinnang: 2

Mõju: Smart-ID-d ei saa kasutada need kasutajad, kelle nutiseadme operatsioonisüsteemile ei ole loodud tuge Smart-ID-le.

Tõenäosus: Riski avaldumine on võimalik, kuid puudutab vaid mõningaid nutiseadmeid, millele pole tuge loodud. Siiani ei ole Smart-ID *app* saadaval Windows Phone operatsioonisüsteemidele [100].

Risk 4: Smart-ID-d ei ole võimalik kasutada ilma internetiühenduseta [100].

Hinnang: 2

Mõju: Smart-ID-d ei saa kasutada autentimiseks või digitaalseks allkirjastamiseks e-teenustes, kui nutiseadmel puudub internetiühendus.

Tõenäosus: Riski avaldumine on võimalik, kuid praktikas on juhtumid harvad.

Risk 5: Smart-ID-d saab kasutada vaid nutitelefoni või tahvelarvuti omanik [101].

Hinnang: 2

Mõju: Smart-ID-d ei saa kasutada need kasutajad, kellel ei ole nutitelefoni või tahvelarvutit.

Tõenäosus: Riski avaldumine on võimalik, kuid praktikas harvad juhtumid.

7.2.5 Riskianalüüsi järeldused

Kõige suurematekс riskideks ID-kaardi puhul on: veebitarkvara kiire ja pideva arenguga veebilehitsejalt ID-kaardi toe kadumine - kõikide operatsioonisüsteemidega ei ole võimalik ID-kaardi tarkvara kasutada. Mobiil-ID suuremaks riskiks on see, et Mobiil-ID kasutamine välismaal võib tuua kaasa suure telefoniarve. Digi-ID puhul on samuti suurematekс riskideks: veebitarkvara kiire ja pideva arenguga veebilehitsejalt Digi-ID toe kadumine ning see, et kõikide operatsioonisüsteemidega ei ole võimalik ID-kaardi tarkvara kasutada. Smart-ID suurematekс riskideks on: paljudes veebikeskkondades ei ole võimalik kasutajal end tuvastada Smart-ID-ga, kuna loodud on vaid ID-kaardi ja Mobiil-ID tugi, Smart-ID-d ei saa kasutada digitaalseks allkirjastamiseks, kui on tegu infovahetuses riigiga.

7.3 Kasutajate analüüs

Internetiküsimustiku läbiviimiseks kasutati internetis saadaval olevat Google Forms-i [112].

Peamine eesmärk internetiküsitluse läbiviimiseks oli koguda võimalikult paljude kasutajate käest informatsiooni, milliseid eID vahendeid nad kõige rohkem kasutavad ning milleks.

See alapeatükk on jagatud kahte osasse. Esimeses osas esitatakse küsimustik. Küsimustiku vastuste analüüs on esitatud teises osas koos küsimustiku tulemuste diagrammidega.

7.3.1 Küsimustik

Küsimustik koosneb 7 küsimusest, millest 6 küsimust on valikuvariantidega ja 1 avatud vastusega küsimus, mis on mittekohustuslik.

Küsimused:

1. **Millist eID vahendit enim kasutate?**
    - ID-kaart
    - Mobiil-ID
    - Smart-ID
    - Digi-ID
    - Ei kasuta üldse
    - *„Other“*
2. **Milleks kasutate kõige rohkem eID vahendeid?**
    - Veebilehekülgedele sisselogimiseks
    - Digiallkirjastamiseks
    - Krüpteerimiseks
    - Kliendikaardina
    - Läbipääsusüsteemides (ID-kaarti ukse avamiseks)
    - *„Other“*
3. **Mis võiks olla teisiti seoses elektroonilise identiteediga?**
    -

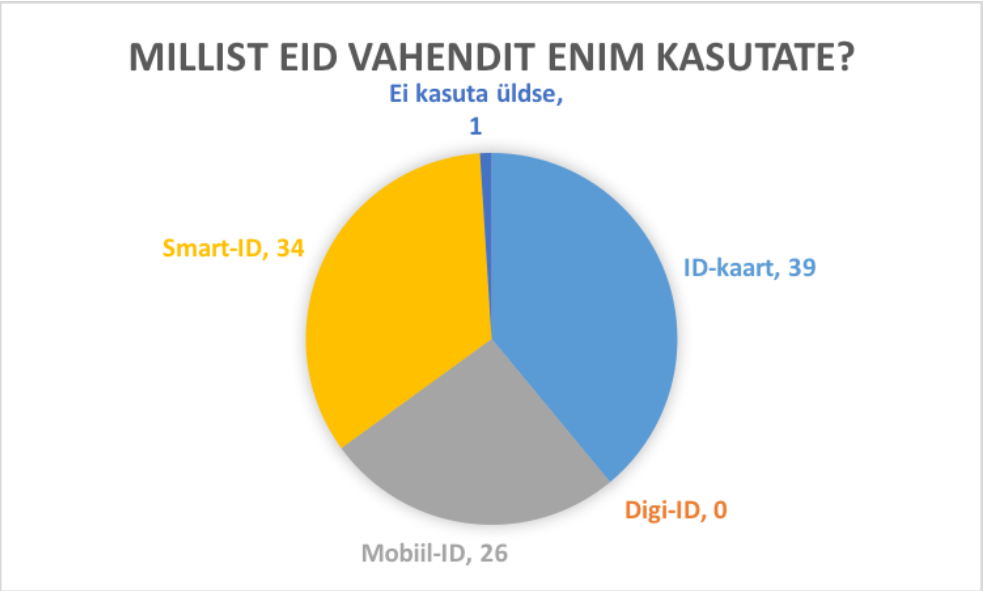
4. **Arvutikasutamise oskus**
    - Väga harv kasutaja
    - Tavakasutaja
    - Professionaalne kasutaja
5. **Teie haridustase**
    - Algharidus
    - Põhiharidus
    - Keskharidus
    - Kõrgharidus
6. **Vanus**
    - kuni 14
    - 15-20
    - 21-30
    - 31-40
    - 41-50
    - 51+
7. **Sugu**
    - Naine
    - Mees

7.3.2 Küsimustiku vastuste analüüs

Küsimustikule vastas 100 inimest.

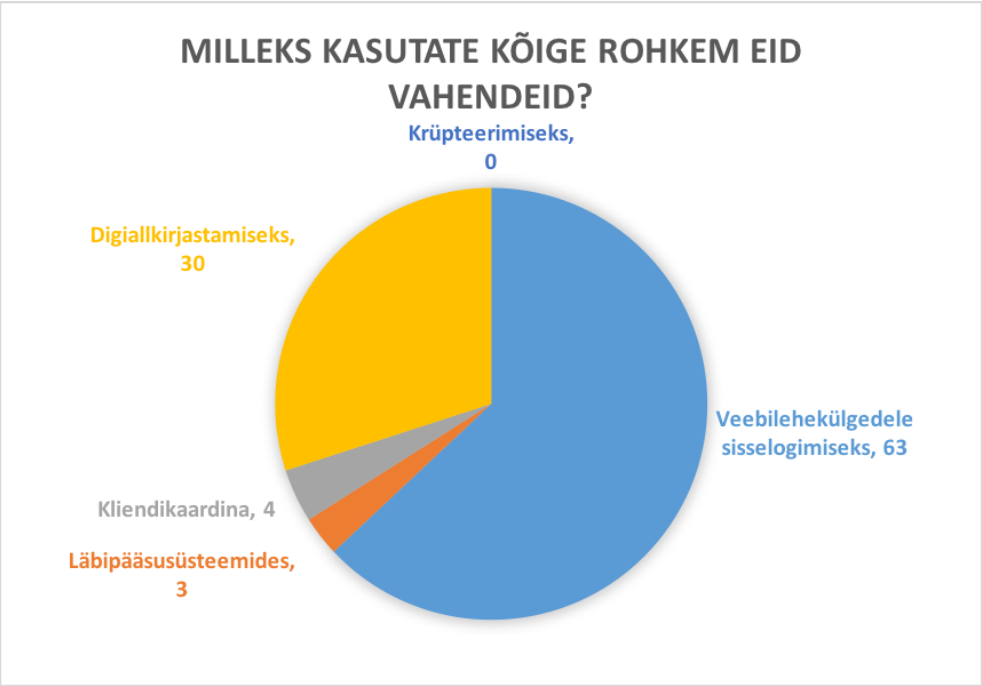
Küsimustik viidi läbi ajavahemikus 19.04 – 21.04.

Allpool on esitatud diagrammid, millel on näha iga küsimuse vastuseid. Diagrammid (Joonis 1-6) on täpsemalt selgitatud diagrammide all ning selle osa lõpus.



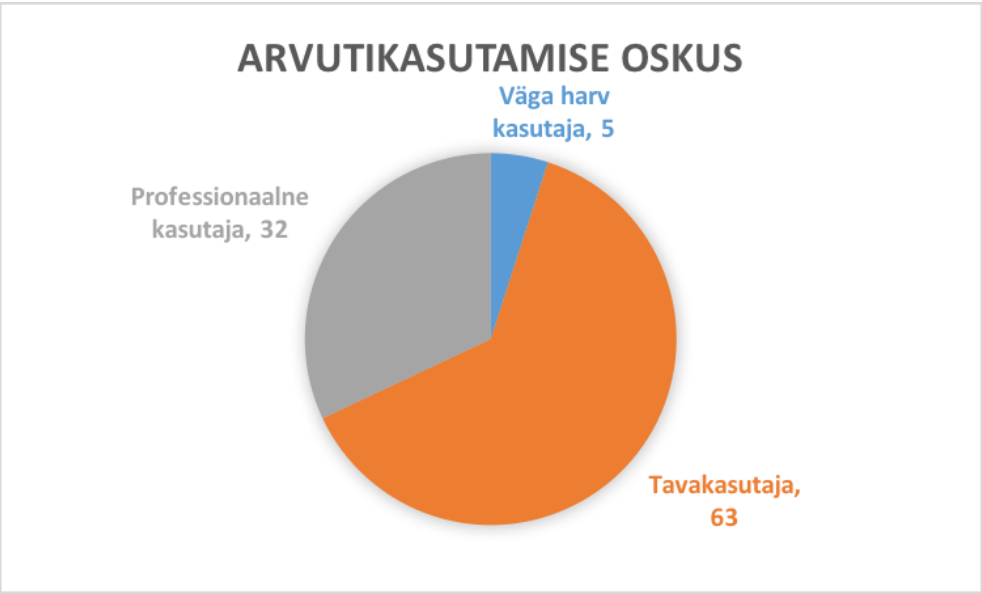
Joonis 1. Küsimus “Millist eID vahendit enim kasutate?”.

Kõige populaarsem eID vahend oli ID-kaart. 39% vastajatest kasutab ID-kaart kõige enam. ID-kaardile järgneb Smart-ID, mida kasutab 34% kasutajatest. Mobiil-ID kasutajaid on vähem, 26% vastajatest kasutab seda. Samuti selgus, et 1 inimene ei kasuta üldse eID vahendeid ning Digi-ID kasutajaid ei olnud ühtegi.



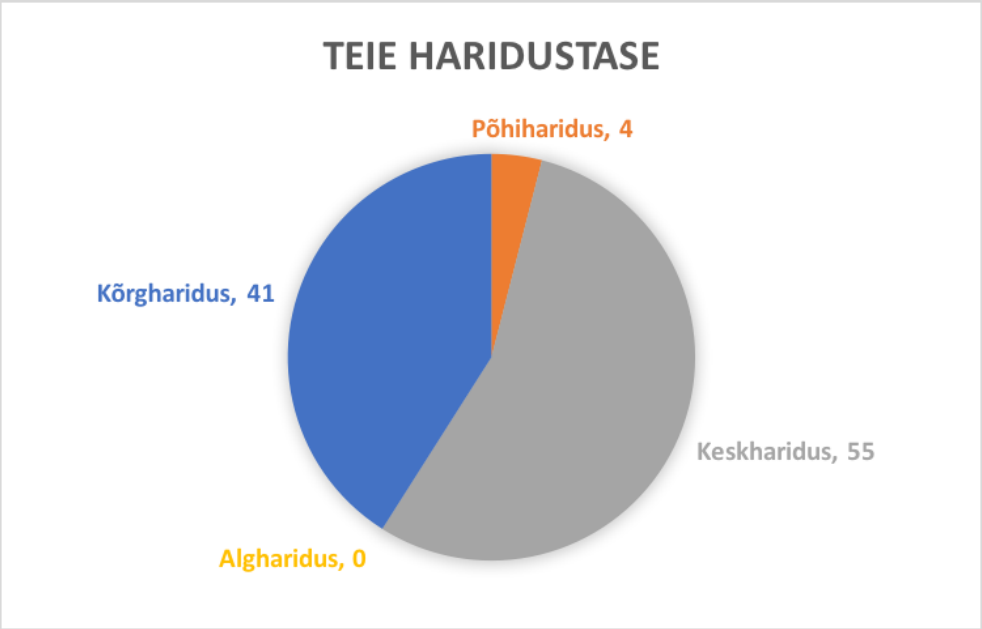
Joonis 2. Küsimus “Milleks kasutate kõige rohkem eID vahendeid?”.

Kõige rohkem kasutavad vastajad eID vahendit elektrooniliseks isikutuvastuseks – 63%. Digitaalset allkirjastamist kasutavad 30% vastajatest kõige rohkem. Vähem kasutatakse eID vahendit kliendikaardina – 4% ja läbipääsusüsteemides – 3%. Küsimustiku vastustest selgus ka, et ükski vastaja ei kasuta eID vahendeid kõige rohkem krüpteerimiseks.



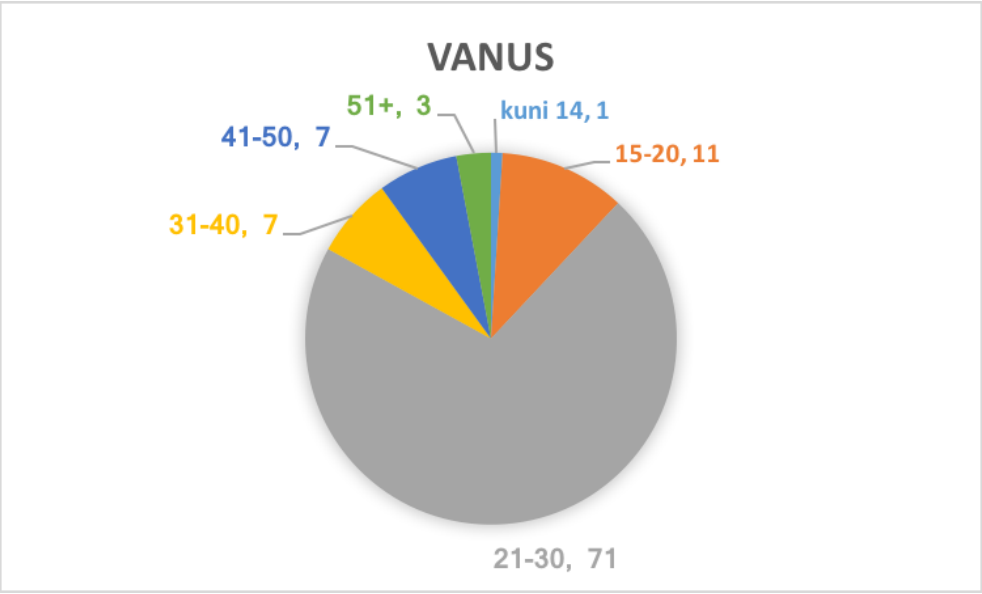
Joonis 3. Küsimus “Arvutikasutamise oskus”.

63% vastajatest olid arvutikasutamise oskuse poolest tavakasutajad. 32% professionaalsed kasutajad ning 5% väga harvad kasutajad.



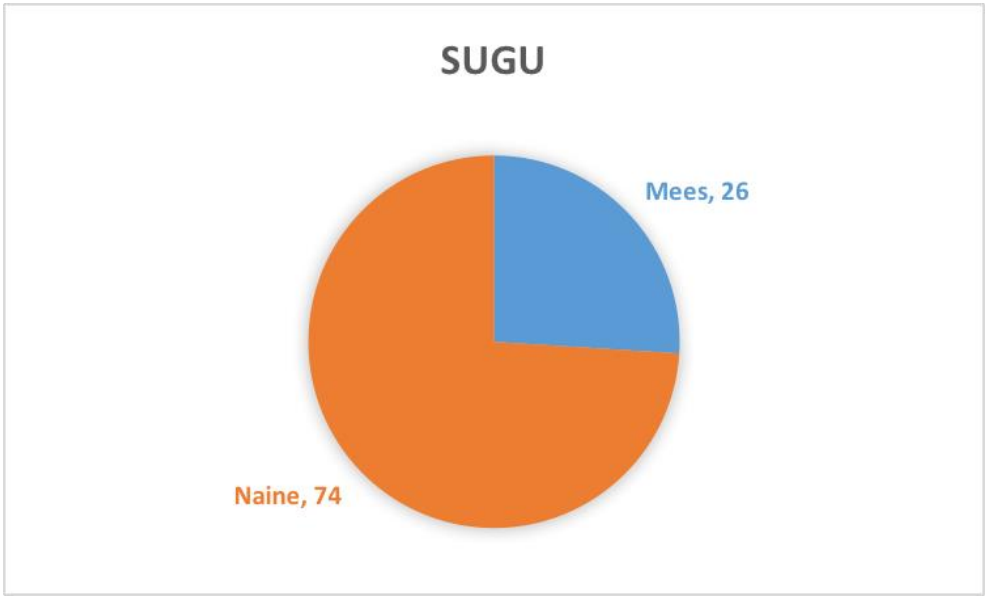
Joonis 4. Küsimus “Teie haridustase”.

55% vastajatest olid keskharidusega, 41% kõrgharidusega ning 4% põhiharidusega. Algharidusega ei olnud ükski vastajatest.



Joonis 5. Küsimus “Vanus”.

71% vastajatest olid 21-30 aastased, 11% 15-20 aastased, 31-40 ning 41-50 aastaseid vastajaid oli 7%, üle 51 aastaseid 3 ning kuni 14 aastaseid 1%.



Joonis 6. Küsimus “Sugu”.

74% vastajatest olid naised ning 26% mehed..

Küsimusele, et mis võiks olla teisiti seoses elektroonilise identiteediga, tõid kasutajad välja, et Mobiil-ID tegemine võiks käia ilma SIM-kaarti vahetamata, ID-kaardi tarkvara peab liiga tihti uuendama. Lisaks tõid mitmed ID-kaardi kasutajad välja, et tarkvara võiks olla töökindlam veebilehitsejates, kuna esineb tihti tõrkeid ID-kaardi kasutamisel. Mitmed Smart-ID kasutajad tõid välja, et Smart-ID-d võiks saada kasutada igal pool veebilehekülgedel ning Smart-ID võiks võrdsustuda Mobiil-ID-ga.

Küsimustiku vastuste analüüsi käigus selgus, et elektrooniliseks isikutuvastuseks kasutatakse kõige rohkem Smart-ID - 29 inimest 63-st. Digitaalseks allkirjastamiseks kasutavad enam kui pooled isikud ID-kaarti: 30-st - 16 inimest. Samuti selgus, et 4% kasutajatest kasutab ID-kaarti läbipääsusüsteemides ning 3% ka kliendikaardina. Selgus ka see, et noored inimesed, 21-30 aastased, kasutavad kõige rohkem Smart-ID-d. Vanemate inimeste seas oli populaarsemad ID-kaart ja Mobiil-ID.

Kokkuvõtvalt võiks välja tuua selle, et kuigi paljud kasutajad tõid välja selle, et Smart-ID-d võiks saada kasutada kõikjal veebilehekülgedel ning et Smart-ID võiks võrdsustuda Mobiil-ID-ga, kasutavad noored kasutajad siiski Smart-ID-d kõige rohkem elektrooniliseks isikutuvastamiseks.

8 Kokkuvõte

Lõputöö eesmärgiks oli selgitada elektroonilise identiteedi olemus ning kuidas see on Eestis alguse saanud ning levinud ja anda ülevaade erinevatest elektroonilise identiteedi vahenditest ja kasutusaladest. Teostada erinevate elektroonilise identiteedi vahendite ja nende kasutusalade analüüs. Eesmärkide saavutamiseks uuriti erinevaid allikaid, koostati autori poolt SWOT – analüüs, riskianalüüs ja internetiküsitlus elektroonilise identiteedi kasutajate seas.

Lõputöö tulemusena:

1. Defineeriti elektroonilise identiteedi olemus ja tutvustati kuidas sai eID alguse Eestis.
2. Anti ülevaade erinevatest elektroonilise identiteedi vahenditest ja kasutusaladest.
3. Anti ülevaade mõningatest välismaal kasutatavatest elektroonilise identiteedi vahenditest.
4. Teostati elektroonilise identiteedi vahendite ja kasutusalade analüüs:
    4.1. SWOT – analüüs tehti erinevatele elektroonilise identiteedi vahendite seas, millega selgitati vahendite võimalused, ohud, nõrkused ja tugevused.
    4.2. Tehti riskianalüüs, milles kasutati SWOT – analüüsis selgunud ohte.
    4.3. Internetiküsitlus viidi läbi elektroonilise identiteedi kasutajate seas.

Töös püstitatud eesmärgid saavutati. Analüüsi osas soovis autor läbi viia ka intervjuud erinevate e-teenuste pakkujate seas, et selgitada välja, milliseid vahendeid nende e-teenustes kasutajad kõige rohkem kasutavad. Kahjuks ei nõustunud ükski valimis olnud asutus intervjuu küsimustele vastama, seetõttu jäeti antud osa lõputööst välja. Kokkuvõtvalt võib öelda, et antud töö annab hea ülevaate elektroonilise identiteedi olemusest, erinevatest vahenditest ja kasutusaladest.

Kasutatud kirjandus

[1] „What is eIDAS?,“ [Võrgumaterjal]. Available: https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-eidas. [Kasutatud 03 04 2018].

[2] „Digi-ID ja ID-tarkvara uuenevad: mida võiksid teada,“ [Võrgumaterjal]. Available: http://forte.delfi.ee/news/digi/digi-id-ja-id-tarkvara-uuenevad-mida-voiksid-teada?id=70726373. [Kasutatud 03 04 2018].

[3] „Võtame ID-kaardi ökosüsteemi osadeks lahti,“ [Võrgumaterjal]. Available: https://geenius.ee/uudis/votame-id-kaardi-okosusteemi-osadeks-lahti/. [Kasutatud 08 04 2018].

[4] „Mis vahe on .ddoc, .bdoc ja .asice formaadis digiallkirjastatud dokumendil?,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=37026. [Kasutatud 24 03 2018].

[5] „ID-kaardi tarkvara uueneb,“ [Võrgumaterjal]. Available: https://blog.ria.ee/tag/eidas/. [Kasutatud 03 04 2018].

[6] „Digidoc failivormingud: DDOC, BDOC, CDOC,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30289. [Kasutatud 24 03 2018].

[7] „Mõisted,“ [Võrgumaterjal]. Available: https://www.ria.ee/teejuht/moisted/#P. [Kasutatud 03 04 2018].

[8] „Elektrooniline identiteet,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/elektrooniline-identiteet.html. [Kasutatud 17 03 2018].

[9] „Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,“ [Võrgumaterjal]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=EN. [Kasutatud 03 04 2018].

[10] „Euroopa Parlamendi ja Nõukogu direktiiv 1999/93/EÜ, 13. detsember 1999, elektroonilisi allkirju käsitleva ühenduse raamistiku kohta,“ [Võrgumaterjal]. Available: http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:31999L0093&from=EN. [Kasutatud 03 04 2018].

[11] „Digitaalallkirjade jätkusuutlikkuse analüüs,“ [Võrgumaterjal]. Available: https://www.id.ee/public/Digitaalallkirjade_jatkusuutlikkuse_analyys.pdf. [Kasutatud 21 03 2018].

[12] „Digitaalallkirja seadus,“ [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/694375. [Kasutatud 18 03 2018].

[13] „Elektroonilise identiteedi kasutusala,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/pki-kasutusala.html. [Kasutatud 28 03 2018].

[14] „Seminar digitaalallkirja rakendamisest Eestis,“ [Võrgumaterjal]. Available: https://sk.ee/uudised/seminar-digitaalallkirja-rakendamisest-eestis. [Kasutatud 21 03 2018].

[15] „Seadusliku digitaalallkirja rakendamise aeg Eestis on saabumas,“ [Võrgumaterjal]. Available: https://sk.ee/uudised/seadusliku-digitaalallkirja-rakendamise-aeg-eestis-on-saabumas. [Kasutatud 21 03 2018].

[16] „Sertifitseerimiskeskus ja Siseministeerium sõlmisid ID kaartide sertifitseerimisteenuse ja väljastamise alase lepingu,“ [Võrgumaterjal]. Available: https://sk.ee/uudised/sertifitseerimiskeskus-ja-siseministeerium-solmisid-id-kaartide-sertifitseerimisteenuse-ja-valjastamise-alase-lepingu. [Kasutatud 21 03 2018].

[17] „Sertifitseerimiskeskus tõi välja digiallkirjastamise klientprogrammi,“ [Võrgumaterjal]. Available: https://sk.ee/uudised/sertifitseerimiskeskus-toi-valja-digiallkirjastamise-klientprogrammi. [Kasutatud 21 03 2018].

[18] „Regulation (Eu) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,“ [Võrgumaterjal]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN. [Kasutatud 03 04 2018].

[19] „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,“ [Võrgumaterjal]. Available: http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32014R0910&from=EN. [Kasutatud 03 04 2018].

[20] „Seadusandlus,“ [Võrgumaterjal]. Available: https://sk.ee/repositoorium/seadusandlus/seadusandlus. [Kasutatud 28 03 2018].

[21] „Jõustus uus digitaalallkirja regulatsioon,“ [Võrgumaterjal]. Available: http://www.rmp.ee/uudised/maksud/joustus-uus-digitaalallkirja-regulatsioon-2016-10-31. [Kasutatud 24 03 2018].

[22] „eID lühitutvustus,“ [Võrgumaterjal]. Available: https://eid.eesti.ee/index.php/EID_l%C3%BChitutvustus. [Kasutatud 17 03 2018].

[23] „ID-kaardi taotlemine täiskasvanule,“ [Võrgumaterjal]. Available: https://www.politsei.ee/et/juhend/id-kaardi-taotlemine-taeiskasvanule/3. [Kasutatud 17 03 2018].

[24] „ID-kaardi taotlemine täiskasvanule,“ [Võrgumaterjal]. Available: https://www.politsei.ee/et/juhend/id-kaardi-taotlemine-taeiskasvanule. [Kasutatud 17 03 2018].

[25] „PIN-koodid,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30242. [Kasutatud 03 04 2018].

[26] „Isikutunnistuse vorm ja tehniline kirjeldus ning isikutunnistusele kantavate andmete loetelu ja isikutunnistusele kantavate digitaalsete andmete kehtivusaeg,“ [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/103122015016. [Kasutatud 17 03 2018].

[27] „ID-kaart ja Digi-ID,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30056. [Kasutatud 17 03 2018].

[28] „Esimesed ID-kaardid inimestel käes,“ [Võrgumaterjal]. Available: https://sk.ee/uudised/esimesed-id-kaardid-inimestel-kaes. [Kasutatud 21 03 2018].

[29] „ID-kaart tähistab 15. sünnipäeva,“ [Võrgumaterjal]. Available: http://www.ega.ee/et/uudised/id-kaart-tahistab-15-sunnipaeva/. [Kasutatud 23 03 2018].

[30] „Mis on sertifikaadid,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30228. [Kasutatud 23 03 2018].

[31] „ID-kaart,“ [Võrgumaterjal]. Available: https://www2.politsei.ee/et/nouanded/dokumentide-naidised/id-kaart/. [Kasutatud 23 03 2018].

[32] „ID-kaardi kiibis avastati turvarisk,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/id-kaardi-kiibis-avastati-turvarisk.html. [Kasutatud 23 03 2018].

[33] „ID-kaardi (Digi-ID ja e-Residendi Digi-ID) sertifikaatide uuendamine - korduma kippuvad küsimused,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30136. [Kasutatud 23 03 2018].

[34] „Uuendati enamik elektrooniliselt kasutatud ID-kaartidest,“ [Võrgumaterjal]. Available: https://www.id.ee/?id=30007&read=38534. [Kasutatud 03 04 2018].

[35] „PPA vahetab välja ligi 12 500 turvanõuetele mittevastavat ID-kaarti,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/ppa-vahetab-valja-ligi-12500-turvanouetele-mittevastavat-id-kaarti.html. [Kasutatud 20 05 2018].

[36] „Mis on Mobiil-ID?,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30057. [Kasutatud 23 03 2018].

[37] „Mobiil-ID taotlemine,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30056. [Kasutatud 17 03 2018].

[38] „Mobiil-ID sertifikaatide uuendamine,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=35897. [Kasutatud 17 03 2018].

[39] [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=36812. [Kasutatud 17 03 2018].

[40] „Tehniline lisainfo,“ [Võrgumaterjal]. Available: https://www.sk.ee/teenused/kehtivuskinnituse-teenus/digidoc-veebiteenus/. [Kasutatud 23 03 2018].

[41] „EMT tõi turule Mobiil-ID teenuse,“ [Võrgumaterjal]. Available: https://sk.ee/uudised/emt-toi-turule-mobiil-id-teenuse. [Kasutatud 21 03 2018].

[42] E. a. M.-I. t. pakkumisega. [Võrgumaterjal]. Available: https://sk.ee/uudised/elisa-alustas-mobiil-id-teenuse-pakkumisega. [Kasutatud 23 03 2018].

[43] „Mobiil-ID ka Tele2 klientidele,“ [Võrgumaterjal]. Available: https://www.id.ee/?id=30011&read=30040&page=20. [Kasutatud 23 03 2018].

[44] „Smart-ID,“ [Võrgumaterjal]. Available: https://www.sk.ee/teenused/smart-id. [Kasutatud 17 03 2018].

[45] „Mis tagab Smart-ID turvalisuse,“ [Võrgumaterjal]. Available: https://www.smart-id.com/et/turvalisus/. [Kasutatud 17 03 2018].

[46] „SK tutvustas uut e-identiteedi lahendust Smart-ID,“ [Võrgumaterjal]. Available: https://sk.ee/uudised/sk-tutvustas-uut-e-identiteedi-lahendust-smart-id. [Kasutatud 21 03 2018].

[47] „Smart-IDd saab tänasest taotleda pangakontorites,“ [Võrgumaterjal]. Available: https://www.sk.ee/uudised/smart-idd-saab-tanasest-taotleda-pangakontorites. [Kasutatud 23 03 2018].

[48] „Smart-ID pälvis Aasta läbimurdja tiitli,“ [Võrgumaterjal]. Available: https://www.sk.ee/uudised/smart-id-palvis-aasta-labimurdja-tiitli. [Kasutatud 23 03 2018].

[49] „Mis on Digi-ID, kuidas seda saada ning mida sellega teha saab,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=34178. [Kasutatud 17 03 2018].

[50] „E-residendi digi-ID,“ [Võrgumaterjal]. Available: https://www.politsei.ee/et/juhend/e-residendi-digi-id. [Kasutatud 08 04 2018].

[51] „Digitaalne isikutunnistus,“ [Võrgumaterjal]. Available: https://sk.ee/teenused/digitaalne-identiteet/digi-id/. [Kasutatud 21 03 2018].

[52] „Riigikogu pikendas digi-ID kehtivusaega viiele aastale,“ [Võrgumaterjal]. Available: http://www.pealinn.ee/tagid/koik/riigikogu-pikendas-digi-id-kehtivusaega-viiele-aastale-n218675. [Kasutatud 21 04 2018].

[53] „ID-kaart,“ [Võrgumaterjal]. Available: https://beta.wikiversity.org/wiki/ID-kaart. [Kasutatud 18 03 2018].

[54] „eID tehniliste funktsioonide lühitutvustus,“ [Võrgumaterjal]. Available: https://eid.eesti.ee/index.php/EID_funktsioonide_l%C3%BChitutvustus_toorik. [Kasutatud 18 03 2018].

[55] „Sertifikaadi kehtivuse kontroll (OCSP),“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30271. [Kasutatud 24 03 2018].

[56] „Kehtivuskinnitusteenus,“ [Võrgumaterjal]. Available: https://www.sk.ee/teenused/kehtivuskinnituse-teenus/. [Kasutatud 24 03 2018].

[57] „Juulist jõustuv Euroopa digimäärus ehk E-Eestist E-Euroopasse,“ [Võrgumaterjal]. Available: http://arileht.delfi.ee/news/uudised/juulist-joustuv-euroopa-digimaarus-ehk-e-eestist-e-euroopasse?id=74913817. [Kasutatud 24 03 2018].

[58] „Statistika,“ [Võrgumaterjal]. Available: https://www.id.ee/. [Kasutatud 21 03 2018].

[59] „Digiallkirjastamine,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30459. [Kasutatud 18 03 2018].

[60] „Riiklikust tarkvarast kaob DDOC-vorming,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/riiklikust-tarkvarast-kaob-ddoc-vorming.html. [Kasutatud 24 03 2018].

[61] „ID-kaardi tarkvaras jääb digitaalallkirja ainsaks vorminguks BDOC,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/id-kaardi-tarkvaras-digiallkirja-ainus-vorming-bdoc.html. [Kasutatud 24 03 2018].

[62] „ID-kaardi tarkvara uuendus toob kaasa mitu olulist muudatust,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/id-kaardi-tarkvara-uuendus-toob-kaasa-mitu-olulist-muudatust.html. [Kasutatud 24 03 2018].

[63] „1. juulist peavad riigiasutused tunnistama teiste EL riikide e-allkirju,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/1-juulist-peavad-riigiasutused-tunnustama-el-riikide-e-allkirju.html. [Kasutatud 18 03 2018].

[64] „Dokumentide krüpteerimine,“ [Võrgumaterjal]. Available: https://www.id.ee/?id=30300. [Kasutatud 18 03 2018].

[65] „ID-kaardi kasutamine kliendikaardina,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30299. [Kasutatud 18 03 2018].

[66] „ID-kaardi kasutamine kliendikaardina,“ [Võrgumaterjal]. Available: https://eid.eesti.ee/index.php/EID_kasutamine_kliendikaardina. [Kasutatud 18 03 2018].

[67] „Apollo Raamatud võttis esimesena ID-kaardi oma kliendikaardiks,“ [Võrgumaterjal]. Available: https://sk.ee/uudised/apollo-raamatud-vottis-esimesena-id-kaardi-oma-kliendikaardiks. [Kasutatud 23 03 2018].

[68] „ID-kaardi kasutamine sissepääsukaardina,“ [Võrgumaterjal]. Available: https://eid.eesti.ee/index.php/ID-kaardi_kasutamine_sissep%C3%A4%C3%A4sukaardina. [Kasutatud 18 03 2018].

[69] „Smart-ID ei võimalda anda omakäelise allkirjaga võrdset digitaalallkirja,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/smart-id-ei-voimalda-anda-omakaelise-allkirjaga-vordset-digitaalallkirja.html. [Kasutatud 08 04 2018].

[70] „Electronic identification,“ [Võrgumaterjal]. Available: https://en.wikipedia.org/wiki/Electronic_identification#Using_the_eID. [Kasutatud 19 04 2018].

[71] „DigiD,“ [Võrgumaterjal]. Available: https://www.iamexpat.nl/expat-info/official-issues/digid-netherlands. [Kasutatud 25 03 2018].

[72] „About DigiD,“ [Võrgumaterjal]. Available: https://www.digid.nl/en/about-digid/. [Kasutatud 25 03 2018].

[73] „Frequently asked questions,“ [Võrgumaterjal]. Available: https://www.digid.nl/en/frequently-asked-questions-about-the-digid-app. [Kasutatud 25 03 2018].

[74] „DigiD for Dutch people living abroad,“ [Võrgumaterjal]. Available: https://www.digid.nl/en/about-digid/digid-for-dutch-people-living-abroad/?color=12345. [Kasutatud 25 03 2018].

[75] „Electronic ID,“ [Võrgumaterjal]. Available: https://www.norge.no/en/electronic-id. [Kasutatud 25 03 2018].

[76] „Information about levels of security,“ [Võrgumaterjal]. Available: http://eid.difi.no/en/security-and-cookies/information-about-levels-security. [Kasutatud 03 04 2018].

[77] „What do I need in order to register a MinID user?,“ [Võrgumaterjal]. Available: http://eid.difi.no/en/what-do-i-need-order-register-minid-user. [Kasutatud 25 03 2018].

[78] „Card issuers,“ [Võrgumaterjal]. Available: https://www.buypass.com/end-user/buypass-id/card-issuers. [Kasutatud 25 03 2018].

[79] „How to log in with Buypass ID on smart card?,“ [Võrgumaterjal]. Available: http://eid.difi.no/en/buypass/how-log-buypass. [Kasutatud 25 03 2018].

[80] „What is NemID?,“ [Võrgumaterjal]. Available: https://international.kk.dk/artikel/what-nemid. [Kasutatud 25 03 2018].

[81] „Introduction to NemID,“ [Võrgumaterjal]. Available: https://www.nemid.nu/dk-en/about_nemid/introduktion_til_nemid/index.html. [Kasutatud 25 03 2018].

[82] „Who can obtain NemID?,“ [Võrgumaterjal]. Available: https://www.nemid.nu/dk-en/about_nemid/who_can_obtain_nemID/. [Kasutatud 25 03 2018].

[83] „About DNIe,“ [Võrgumaterjal]. Available: https://www.signicat.com/eid-world-map/. [Kasutatud 28 03 2018].

[84] „SWOT-analüüs,“ [Võrgumaterjal]. Available: http://www.lvrkk.ee/kristiina/ariplaan/6_swotanals.html. [Kasutatud 30 03 2018].

[85] „SWOT-analüüs nõuab objektiivsust ja süvenemist,“ [Võrgumaterjal]. Available: http://bda.ee/swot-analuus-nouab-objektiivsust-ja-suvenemist/. [Kasutatud 31 03 2018].

[86] „Riskijuhtimise protsess ja riskide hindamise meetodid,“ [Võrgumaterjal]. Available: http://www.siseaudiitor.ee/riskijuhtimise-protsess-ja-riskide-hindamise-meetodid/. [Kasutatud 31 03 2018].

[87] „Küsitlustehnikate võrdlus,“ [Võrgumaterjal]. Available: http://e-ope.khk.ee/oo/evoti/kysitlus/ksitlustehnikate_vrdlus.html. [Kasutatud 03 04 2018].

[88] „The 17 Best Online Form Builder Apps for Every Task,“ [Võrgumaterjal]. Available: https://zapier.com/learn/forms-surveys/best-online-form-builder-software/. [Kasutatud 03 04 2018].

[89] „ID-kaardi PIN-koodid kadunud või ununenud,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30133. [Kasutatud 08 04 2018].

[90] „ID-kaardi kriis maksis ametitele miljoneid,“ [Võrgumaterjal]. Available: https://www.err.ee/693331/id-kaardi-kriis-maksis-ametitele-miljoneid. [Kasutatud 15 04 2018].

[91] „Kuidas saab eelmise ID-kaardi või uuendatud sertifikaadiga krüpteeritud turvaümbrikut avada?,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=34264. [Kasutatud 12 04 2018].

[92] „Kuidas hankida ID-kaarti,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=30219. [Kasutatud 08 04 2018].

[93] „Avaliku võtme infrastruktuur,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/pki.html. [Kasutatud 08 04 2018].

[94] „ID-tarkvara versioonides toetatud op. süsteemid,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=36138. [Kasutatud 17 04 2018].

[95] „Kuidas taotleda Mobiil-IDd?,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=36811. [Kasutatud 08 04 2018].

[96] „Mobiil-ID PIN-koodide vahetamine ja lahti blokeerimine,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=34246. [Kasutatud 08 04 2018].

[97] „Mobiil-ID taotluskeskkond,“ [Võrgumaterjal]. Available: https://taotlus.politsei.ee/. [Kasutatud 18 04 2018].

[98] „Mobiil-ID,“ [Võrgumaterjal]. Available: https://www.elisa.ee/et/eraklient/apid-ja-lisateenused/lisateenused/mobiil-id. [Kasutatud 08 04 2018].

[99] „Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuring,“ [Võrgumaterjal]. Available: https://www.ria.ee/public/toetusskeem/nuti-uuring2017_aruanne.pdf. [Kasutatud 08 04 2018].

[100] „Korduvad küsimused,“ [Võrgumaterjal]. Available: https://www.smart-id.com/et/abi/kkk. [Kasutatud 08 04 2018].

[101] „Smart-ID: Laadi alla äpp & loo konto,“ [Võrgumaterjal]. Available: https://www.smart-id.com/et/laadi-alla/. [Kasutatud 08 04 2018].

[102] „Selline on Eesti uus autentimislahendus Smart-ID, mis töötab ideaalselt mobiilis,“ [Võrgumaterjal]. Available: https://geenius.ee/uudis/selline-eesti-uus-autentimislahendus-smart-id-mis-tootab-ideaalselt-mobiilis/. [Kasutatud 08 04 2018].

[103] „TURVALINE,“ [Võrgumaterjal]. Available: https://www.smart-id.com/et/smart-id/. [Kasutatud 08 04 2018].

[104] „Mis tagab Smart-ID turvalisuse?,“ [Võrgumaterjal]. Available: https://www.smart-id.com/et/turvalisus/. [Kasutatud 08 04 2018].

[105] „E-hääletamise üldkirjeldus,“ [Võrgumaterjal]. Available: https://www.valimised.ee/et/e-h%C3%A4%C3%A4letamine/e-h%C3%A4%C3%A4letamise-%C3%BCldkirjeldus. [Kasutatud 12 04 2018].

[106] „Mida on vaja teha, kui ID-kaardi sertifikaadid on peatatud?,“ [Võrgumaterjal]. Available: https://www.id.ee/?id=30007&read=38350. [Kasutatud 17 04 2018].

[107] „Uues OSX versioonis (10.12, Sierra) ei tööta Safariga eID kaardi kasutamine,“ [Võrgumaterjal]. Available: https://www.id.ee/index.php?id=37798. [Kasutatud 17 04 2018].

[108] „ID-kaardi tarkvara paigaldamine (eellugu),“ [Võrgumaterjal]. Available: https://blog.ria.ee/tag/id-kaart/page/3/. [Kasutatud 17 04 2018].

[109] „Teadlased avalikustasid Eesti ID-kaardi turvariski tehnilise kirjelduse,“ [Võrgumaterjal]. Available: https://www.err.ee/636860/teadlased-avalikustasid-eesti-id-kaardi-turvariski-tehnilise-kirjelduse. [Kasutatud 28 04 2018].

[110] „Mobiili-ID taotluste hulk on päevaga kahekordistunud,“ [Võrgumaterjal]. Available: http://www.pealinn.ee/tagid/koik/mobiili-id-taotluste-hulk-on-paevaga-kahekordistunud-n200575. [Kasutatud 17 04 2018].

[111] „Ettevaatust: mobiil-ID kasutamine välismaal võib põhjustada megaarve,“ [Võrgumaterjal]. Available: https://tehnika.postimees.ee/4379813/ettevaatust-mobiil-id-kasutamine-valismaal-voib-pohjustada-megaarve. [Kasutatud 17 04 2018].

[112] „Looge kauneid vorme,“ [Võrgumaterjal]. Available: https://www.google.com/forms/about/. [Kasutatud 27 04 2018].