Tallinna Ülikool

Informaatika Instituut

EESTI AVALIKU SEKTORI IDENTITEEDI- JA PÄÄSUÕIGUSTE HALDUS

Magistritöö

Autor: Erkki Erend

Juhendaja: Priit Parmakson

Autor: ……..... „ … “ …….. 2011.a.

Juhendaja: …… „ … “ ……...2011.a.

Instituudi juhataja: ……..... „ … “ ……...2011.a.

Tallinn 2011

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....

(kuupäev) (autor)

Saateks

Autor tänab magistritöö juhendajat Priit Parmaksoni pühendumise ja nõuannete eest.

Suurimad tänud uuringus osalenud asutustele ja spetsialistidele, et leidsite aega kohtumiseks ja tutvustasite kannatlikult keerukaid süsteeme ja protsesse.

Suur tänu praegustele ja endistele kolleegidele, kes nõu ja jõuga selle töö valmimist toetasid.

Ilma lähedaste ja sõprade mõistva suhtumiseta poleks selle töö valmimine võimalik olnud, suur aitäh teile kõigile!

ANNOTATSIOON

Käesolev magistritöö uurib ja kirjeldab digitaalse identiteedi mõistet ja sisu, selgitatakse identiteedihalduse mõistet ja pääsuõiguste haldamise mudeleid, tutvustatakse tähtsamaid identiteedi- ja pääsuõiguste süsteeme ja programme Eestis ja Euroopa Liidus. Valimi abil uuritakse Eesti avaliku sektori asutusi ja infosüsteeme pääsuõiguste- ja identiteedihalduse vaatenurgast.

Käesoleva töö eesmärkideks on selgitada identiteedi- ja pääsuõiguste halduse ülesehitust ja hinnata valimi abil Eesti avaliku sektori asutuste pääsuõiguste ja eelkõige identiteedihalduse korraldust. Ühtlasi on töö eesmärgiks selgitada välja parimad praktikad ja nende kasutamine avaliku sektori identiteedihalduse süsteemides.

Märksõnad: digitaalne identiteet, digitaalse identiteedi elutsükkel, identifitseerimine, autentimine, autoriseerimine, pääsuõigused, pääsukontroll, kohustuslik pääsukontroll, diskretsionaarne pääsukontroll, rollipõhine pääsukontroll, identiteedihaldus, identiteedihalduse süsteemid, identiteedihalduse mudelid.

Magistritöö on kirjutatud eesti keeles, koosneb 73 leheküljest, sisaldades 6 peatükki, 22 joonist ja tabelit.

SISUKORD

SISSEJUHATUS

Eesti Vabariik on noor riik nii ajalises kui ka infotehnoloogilises mõistes. Noorus infotehnoloogilises mõistes ei tähenda ilmtingimata nõrkust ja Eesti kontekstis viitab pigem uutele ideedele ning värsketele infotehnoloogilistele lahendustele. Eesti alustas süsteemide ja infrastruktuuri arendamisega sellel ajahetkel kui paljud tehnoloogiad ja vahendid olid just muutunud kasutusküpseks ning omandanud laialt kättesaadava vormi. See on ka üks põhjustest, miks on infotehnoloogia areng Eestis olnud väga kiire. Selle kiire arengu keskmes on ka riigiasutused, kelle hallata on riiklikud andmekogud, mis sisaldavad muuhulgas isiku-andmeid, riigisaladust, maksusaladust ning muud informatsiooni, millele ligipääs peab olema piiratud ning kasutamine tuvastatav. Kõrgendatud nõuded andmekaitsele lisavad riiklikele andmekogudele täiendava mõõtme – andmete turvalisuse. Turvaküsimused, eelkõige aga pääsu reguleerimine ja korraldamine olid pikka aega andmekogude omanike vastutada. Detailsed riiklikult kehtestatud reeglid sisuliselt puudusid. Olid ja on tänaseni olemas küll teatud seadused ja määrused (näiteks 2003. aasta kaitseministri määrus „Elektroonilise teabeturbe ning eriside korraldamiseks ja kontrollimiseks kasutatavad meetodid ja vahendid“[1]), mis esitavad mõningad põhinõuded tundlikke andmeid töötlevatele süsteemidele, kuid auditeeritav süsteem puudus. Olukorra muutis konkreetsemaks riiklik etalonturbesüsteem ISKE[2], mis Saksa riikliku etalonturbesüsteemi järgi tõlgiti ja kohandati Riigi Infosüsteemide Arenduskeskuse poolt alates 2003. aastast ning mis on suunatud riigi ja kohaliku omavalitsuse andmekogudele.

Teema valik on suuresti tingitud autori töötamisest avaliku sektori asutuse IT juhina, kus pääsuõiguste temaatika on tähtsal kohal ning identiteetide haldamise ja parema korraldamisega on tegeletud juba aastaid. Endise süsteemiadministraatorina on autor seisukohal, et kõik tööd, mis kätkevad endas igapäevast rutiinset tööd, tuleks anda üle masinatele ning inimene peaks jääma vaatlevaks ja kontrollivaks organiks. Üheks selliseks rutiiniks on kindlasti identiteetide haldamine ja pääsuõiguste korraldamine.

[1] https://www.riigiteataja.ee/akt/12783356

[2] http://www.ria.ee/iske

Eesmärkide püstitus

Töö eesmärgiks on selgitada identiteedi- ja pääsuõiguste haldusega[3] (edaspidi IPH) seotud mõisteid, meetodeid, poliitikaid ning uurida valitud juhtumiuuringute abil IPH olukorda Eesti avalikus sektoris. Teemavaliku alguspunktiks on identiteedihalduse[4] (edaspidi IH) ja pääsuõiguste halduse[5] (edaspidi PÕH) temaatika järjest aktuaalsemaks muutumine Eesti avalikus sektoris. Mida rohkem on riigi poolt regulatsioone (kaitseministri määrus „Elektroonilise teabeturbe ning eriside korraldamiseks ja kontrollimiseks kasutatavad meetodid ja vahendid", ISKE jt) ja teadlikkust tõstvaid koolitusi andmekaitse osas, seda rohkem pööratakse tähelepanu ka pääsuõiguste korraldamisele. Teisalt aga on välisabina saadud ressursside, struktuurfondide toetuste ja Euroopa Liiduga liitumisega kaasnenud nõuetega süsteemiarendusele intensiivistunud tarkvaraarendus. Selle tulemusena kasvab aasta-aastalt andmekogude ja infosüsteemide arv, mille seas on palju avalikke infosüsteeme ja andmekogusid. Andmekogude ja infosüsteemide arvu kasv loob olukorra, kus infosüsteemide kasutajatel on lisaks nende isiklikele identiteetidele (Skype, MSN, Gmail, Facebook jt) hulk identiteete avalikes infosüsteemides ja andmekogudes. See tähendab, et tähelepanu keskmesse on tõusmas identiteetide haldamisega seonduvad küsimused. Paljudel kodanikel on olemas ID kaart ning eesti.ee e-posti aadress - mõlemad on väga teretulnud vahendid elektroonilises maailmas, kuid nii ID-kaart kui ka eesti.ee e-posti aadress on identiteedid ja vajavad samamoodi haldamist nagu iga teine identiteet. Eesti avalikus sektoris pole uuritud olukorda identiteedihalduse ja pääsuõiguste halduse vallas, sh kasutatavaid lahendusi, nende tugevaid ja nõrku külgi. Puudub ülevaade IPH probleemidest ja sellest, kas identiteedi- ja pääsuõiguste halduses saaks kasutada odavamaid ja paremaid lahendusi ja kas on võimalik tuvastada parimaid praktikaid. Töö eesmärgiks on saada valimi abil piiratud, kuid siiski kasulik ja kasutatav ülevaade Eesti avalikus sektoris kasutatavatest IPH meetoditest ja tehnilistest lahendustest. Lisaks sellele on töö eesmärgiks tuvastada IPH parimad praktikad, tutvustada ja levitada neid käesoleva töö kaudu.

IPH on tugevalt seotud teiste IT valdkondadega, näiteks kasutajaõiguste haldamisega, infoturbega, tarkvara arendamisega jt. Kuna IPH on keeruline ja mahukas infotehnoloogiline teema, siis on selge, et uurimiseesmärke tuleb kitsendada, kuna kõike teemaga seonduvat ei

[3] ingl. *identity and access management (IAM)*

[4] ingl. *identity management*

[5] ingl. *access management*

ole antud magistritöö raames võimalik ega otstarbekas uurida. Teema uurimiseks valitud valim võib tunduda väike ja teema lihtne, kuid tegelikult on teema ulatuslik ja keeruline. Identiteedi- ja pääsuõigustega seonduv eestikeelne terminoloogia on suhteliselt vähearenenud, lahendused ja protsessid on keerulised ning teema varem uurimata. Teoreetilise materjali põhjalik läbitöötamine ning hoolikalt valitud valim peaksid andma piisava ning vajaliku ülevaate identiteedi- ja pääsuõiguste haldusest Eesti avalikus sektoris. Töös plaanitud kogutav teadmus on kokkuvõtlikult väljendatav kahe hüpoteesiga:

Hüpotees 1: Avaliku sektori asutustes rakendatud identiteedi- ja pääsuõiguste halduse lahendused ei ole tänapäevased, nende arendamisel ei ole lähtutud parimatest praktikatest ning identiteedi- ja pääsuõiguste arendamisega avaliku sektori asutustes ei tegeleta piisavalt.

Hüpotees 2: Avaliku sektori asutuste identiteedi- ja pääsuõiguste haldamise taset on võimalik tõsta kui tuvastada ja juurutada parimad praktikad.

Magistritöö struktuur

Esimeses peatükis tutvustab autor digitaalset identiteeti, selle seost turvalisuse ja privaatsusega, digitaalse identiteedi elutsüklit ning selgitab identifitseerimise ja autentimise mõisteid ning sisu.

Teises peatükis annab autor ülevaate digitaalsete identiteetide, identifitseerimise ja autentimise ning autoriseerimise seostest, selgitab pääsuõiguste ja autoriseerimise seoseid ning tutvustab pääsuõiguste poliitikaid, sh rollipõhist pääsupoliitikat.

Kolmandas peatükis selgitab autor identiteedihalduse mõistet ning identiteedihalduse seost identiteedihaldussüsteemidega, ühtlasi tutvustab erinevaid identiteedi mudeleid ning olulisemaid tehnilisi lahendusi.

Neljandas peatükis tutvustab autor identiteedi- ja pääsuõiguste halduse suuremaid projekte Eestis ja Euroopa Liidus.

Viiendas peatükis tutvustab autor empiirilise andmestiku kogumiseks küsitletud asutusi ning infosüsteeme.

Kuuendas peatükis analüüsib autor juhtumiuuringutes saadud materjali abil hüpoteese, tutvustab leitud parimaid praktikaid identiteedi- ja pääsuõiguste halduses, analüüsib nende praktikate rakendamist ning teeb ettepanekuid analoogsete uuringute läbiviimise kohta.

1. DIGITAALNE IDENTITEET

Et aru saada, mis on identiteedi- ja pääsuõiguste haldus, on esmalt vaja selgitada digitaalse identiteedi mõiste. Digitaalse identiteedi mõiste, nagu IPH temaatika üldiselt, on abstraktne ning pole üks-üheselt kõigile arusaadav. Paljud IT spetsialistid ja IT juhid peavad digitaalset identiteeti samaks kasutajakontoga ning ei pea kasutajakonto ja digitaalse identiteedi mõistete vahe tegemist oluliseks. Selle vahe mõistmine on aga tähtis, et aru saada identiteedi- ja pääsuõiguste haldusest kui tervikust. Järgnevalt selgitatakse, mis on digitaalne identiteet, kuidas see tekib, millest koosneb ning millised on selle seosed autentimis- ja identifitseerimisprotsessiga.

Digitaalse identiteedi mõistet on lahti mõtestatud mitmeti, kuid kõige täpsem oleks ehk järgmine: *„Digitaalne identiteet on unikaalsete andmete kogum, mis kirjeldab isikut või eset, ehk subjekti või olemit digitaalses maailmas ning ühtlasi sisaldab andmeid subjekti suhete kohta teiste olemite ning subjektidega“*. (Windley, 2005) Näitena võib tuua auto andmed, mis kogutakse Maanteeameti poolt hallatavasse Liiklusregistrisse. Auto kohta on seal ilmselt olemas VIN kood[6], mida võidakse kasutatakse unikaalse tunnusena. Lisaks sellele on registris andmed auto mudeli, tüübi, massi, värvi jne kohta. Auto seoste osas teiste subjektide või olemitega on registris olemas andmed omaniku ning eelmiste omanike kohta. Kõik need autoga seonduvad andmed ja seosed moodustavad auto digitaalse identiteedi. Digitaalse identiteedi haldamine on seotud identiteedi loomise, uuendamise, kasutamise ja kõige lõpuks hävitamisega. Ilmselt hävitab või eemaldab ka Maanteeamet teatud aja tagant Liiklusregistrist aegunud andmeid. Analoogsed andmed võivad identifitseerida isikut, arvutit, maatükki või ükskõik millist muud subjekti või olemit. Vahel luuakse selliseid andmeid registritesse lihtsalt selleks, et nende üle saaks arvestust pidada, kuid antud magistritöö fookuses on need andmed, mille loomisel on peetud silmas ligipääsude andmist või võtmist, näiteks hoonesse või arvutisüsteemi. Seosed identiteetide ja lubatud tegevuste vahel on digitaalses maailmas vajalikud ning kasulikud, kuid ühtlasi väga raskelt hallatavad.

Digitaalse identiteediga seondub hulk termineid, mis vajavad samuti selgitamist. Subjekt võib olla isik, organisatsioon, programm, masin või mingi muu asi, mis soovib ressursile ligipääsu. Ressurss võib olla veebileht, fail kõvakettal, andmekogum andmebaasis vms. Et saada ligipääs ressursile, väidab subjekt end olevat keegi (omab teatud identiteeti). Kuna ressursse

[6] ingl. *vehicle identification number*

kasutavad ka süsteemid ja programmid, siis kasutatakse digitaalses maailmas sõna isik asemel sõna subjekt. Digitaalse identiteedi kontekstis on identiteedid andmekogumid subjektide kohta, mille võib tinglikult jagada kolmeks grupiks - atribuudid[7], eelistused[8] ja tunnusjooned[9]. Atribuudid luuakse, kirjeldades informatsiooni subjekti kohta, näiteks nagu terviseandmed, ostukäitumine, pangaarvel olev summa, riiete suurus, vanus jne. Eelistused näitavad soove, näiteks eelistused istekoha osas kinos, hot-dogi lemmiktüüp, eelistatud valuuta jne. Tunnusjooned on nagu atribuudid, subjektile iseloomulikud jooned, kuid need on olemas või „kaasa sündinud". Tunnusjoonteks võivad näiteks inimesel olla sinised silmad, ettevõtte puhul kuidas ja millal on ettevõte loodud. Üldjuhul tunnusjooned ei muutu, muutuvad atribuudid. (Windley, 2005)

1.1. Digitaalne identiteet, turvalisus ja privaatsus

Digitaalse identiteedi temaatikat peetakse tihti infoturbe alamteemaks. Digitaalne identiteet on kindlasti oluline turvalisuse komponent, kuid digitaalsel identiteedil on rohkem kasutusalasid kui pelgalt info kaitse.

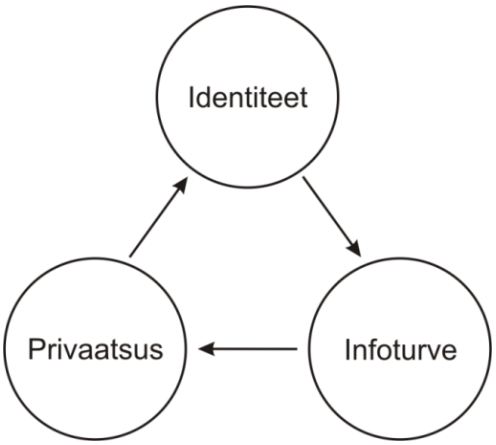
Infoturve on teabe ja infosüsteemide kaitsmine loata juurdepääsu, kasutamise, avaldamise, muutmise või hävitamise eest. (Portaal arenguhuvilisele juhile, 2011)

Andmekaitse ja infoturbe seletussõnastik (Hanson, Laur, Buldas, & Nõgisto, 2011) selgitab, et privaatsus on isiku või rühma võime soovitud ulatuses isoleerida teistest ennast või teavet enda kohta, avalikustades end valikuliselt; privaatseks loetava piirid ja sisu erinevad kultuuriti ja isikuti. Digitaalse identiteedi vaatenurgast on privaatsus identiteediga seonduvate atribuutide, eelistuste ja tunnusjoonte kaitse selle eest, et need ei leviks rohkem kui subjektile vajalik. Privaatsus toetub infoturbele, mis omakorda toetub digitaalse identiteedi infrastruktuurile, nagu on näha jooniselt 1. (Windley, 2005)

[7] ingl. *attributes*

[8] ingl. *preferences*

[9] ingl. *traits*



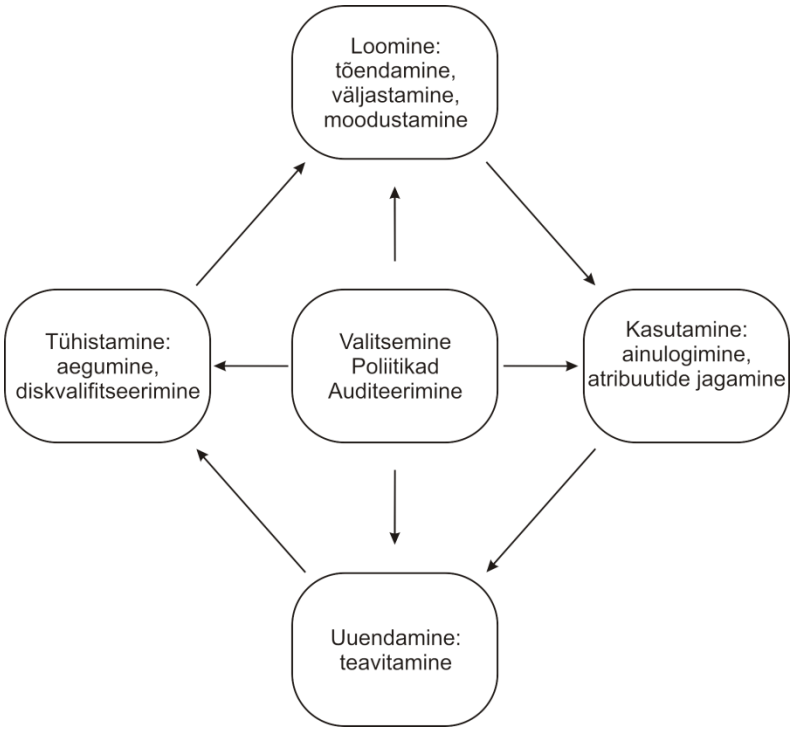
Joonis 1. Identiteedi, privaatsuse ja infoturbe suhe. (Windley, 2005)

1.2. Digitaalse identiteedi elutsükkel

Digitaalse identiteedi eluiga nimetatakse elutsükliks. Digitaalsed identiteedid vajavad kogu elutsükli jooksul korraldamist. Identiteedihalduse üheks eesmärgiks on tegeleda digitaalse identiteedi elutsükli korraldamisega, alates loomisest kuni tühistamiseni[10]. Digitaalse identiteedi elutsüklit toetab ja juhib valitsemine[11]. Elutsükkel ise koosneb neljast faasist: loomine, kasutamine, uuendamine ja tühistamine (Bertino & Takahashi, 2011). Elutsüklit iseloomustab joonis 2:

[10] ingl. *revocation*

[11] ingl. *governance*



Joonis 2. Identiteedi elutsükkel (Bertino & Takahashi, 2011)

Digitaalse identiteedi elutsükli mudeli selline kujutamine, on laialt levinud ning leidub lisaks viidatud allikale ka mitmetes teistes allikates. Näiteks raamatus «Digital Identity» (Windley, 2005) kujutatakse digitaalse identiteedi elutsüklit väga sarnaselt joonisele 2.

1.2.1. Loomine

Digitaalse identiteedi elutsükkel saab alguse selle loomisest[12]. Digitaalse identiteedi loomist nimetatakse identiteedihaldussüsteemide kontekstis ka provisjoneerimiseks[13]. (Windley, 2005) Digitaalse identiteedi loomine koosneb kolmest sammust: atribuutide tõendamine, mandaadi[14] väljastamine ja identiteedi moodustamine.

Atribuutide tõendamine tähendab atribuutide saaja jaoks usaldusväärse allika kinnitust atribuutide õigsuse kohta. Näiteks sünniaeg on kinnitatud kohaliku omavalitsuse poolt välja antava sünnitunnistusega. Atribuutide tõendamise asjaolud peavad atribuutide saajale kättesaadavad ja selged olema, et saaja saaks hinnata atribuutide usaldusväärsust.

[12] ingl. *creation*

[13] ingl. *provisioning*

[14] ingl. *credentials*

Mandaadi[15] **väljastamine** toimub usaldusväärse institutsiooni poolt peale seda kui atribuudid on tõendatud. Mandaat võib esineda mitmel erineval kujul, näiteks digitaalse sertifikaadi, parooli ja/või sõrmejälje kujul. Mandaadi määramise asjaolud peavad mandaadi saajale kättesaadavad ja selged olema, et saaja saaks hinnata mandaadi usaldusväärsust. Asjaolude hulka kuuluvad ka andmed mandaadi väljastaja kohta, mandaadi väljastamise aeg ning aegumise tähtaeg.

Identiteedi moodustamine tähendab seda, et identiteet vormistatakse tõendatud atribuutide, väljastatud mandaatide ning muude identifikaatorite põhjal, mille määrab subjekt või kolmandad osapooled. (Bertino & Takahashi, 2011) Identiteedi moodustamine tähendab seda, et kõik vajalikud andmed identiteedi kirjeldamiseks on kogutud ning see kogum on sisestatud identiteedi haldamisega tegelevasse süsteemi, et saaks alata identiteedi elutsükli järgmine etapp – identiteedi kasutamine.

1.2.2. Kasutamine

Moodustatud identiteete võib kasutada mitmeti, kuid mis kõige tähtsam, neid peab kasutama selliselt, et oleks tagatud identiteetide turvalisus ja privaatsus. Tuntakse kolme põhilist identiteetide kasutamise funktsiooni: usaldusväärne kommunikatsioon, ainulogimine[16] ja atribuutide jagamine.

Usaldusväärses kommunikatsioonis peavad sõnumite saatjad ja vastuvõtjad olema võimelised tuvastama, eristama ja kinnitama identiteetide autentsust usaldusväärsel moel. Seega on usaldusväärsed identiteedid usaldusväärse kommunikatsiooni aluseks. (Bertino & Takahashi, 2011)

Ainulogimine on identiteedi ülekanne võimaldades subjektil taaskasutada autentimise tulemit ligipääsul mitmetele ressurssidele või teenustele. Lihtsustades tähendab see seda, et kui subjekt on end korra juba autentinud ja on olemas toimiv ainulogimise lahendus, mis kannab identiteedi üle ühest süsteemist teise, siis pole subjektil vaja autentimise tegevust korrata.

Atribuutide jagamine on transaktsioon[17], mis võimaldab identiteeti pakkuvatel osapooltel jagada subjektide kohta käivaid atribuute. Identiteeti pakkuvateks osapoolteks võivad olla

---

[15] ingl. *credentials,* olemi (näiteks kasutaja või süsteemi) väidetava identiteedi tõendamiseks (autentimiseks) edastatavad andmed (näiteks parool) (Hanson, Laur, Buldas, & Nõgisto, 2011)

[16] ingl. *single sign on*

[17] ingl. *transaction*

erinevad identiteedihalduse süsteemid, kus asuvad identiteedi kohta erinevad atribuudid. Kui atribuudid on aga hajutatud mööda erinevaid süsteeme ja osapooli, siis see võib luua atribuutide liiasuse ning ebakõla. Atribuutide liiasus identiteedi kontekstis ei ole positiivne omadus, selle leevendamiseks on olemas erinevad meetodid, näiteks metakataloogid ja virtuaalkataloogid. Erinevates infosüsteemides küsitakse kasutaja käest elukoha andmeid, atribuutide jagamise tulemusena poleks see aga vajalik. Andmete mitteküsimisel on korrektne nende andmete saamine teiste identiteeti pakkuvate osapoolte käest kasutajaga kooskõlastada.

1.2.3. Uuendamine

Identiteetide kohta käivaid andmeid on vaja elutsükli jooksul pidevalt uuendada. Näiteks aeguvad väljaantud sertifikaadid, paroolid ning mõned atribuudid muutuvad ajas, näiteks isiku terviseandmed. Et tagada identiteedi terviklus, tuleb identiteediga seonduvaid andmeid korrapäraselt uuendada. Identiteediga seonduvaid andmeid uuendatakse tavaliselt käsitsi, vahel ka automaatselt. Hea praktika on see, et identiteetidega seonduvad andmed uuendatakse käsitsi ühe korra ning nende edastamine erinevatesse süsteemidesse toimub automaatselt. (Bertino & Takahashi, 2011)

1.2.4. Tühistamine

Kui identiteedid ja mandaadid vananevad ja/või muutuvad kehtetuks, on vaja need tühistada. Tühistamist nimetatakse erinevates allikates identiteedihaldussüsteemide kontekstis ka deprovisjoneerimiseks[18]. (Windley, 2005) Autentimine ja autoriseerimine toetuvad identiteedi andmetele ning tagamaks nende kehtivust, on äärmiselt oluline identiteetide ja mandaatide tühistamise protsess. Näiteks töötaja töölt lahkumisel on tavaliselt vajalik kohe ligipääsud sulgeda, mandaadid tuleb tühistada niipea kui need on aegunud, varastatud või muudmoodi ohustatud. Tühistamisega seonduvat informatsiooni on vaja omakorda osapoolte vahel jagada, et tagada andmete terviklus. (Bertino & Takahashi, 2011)

1.2.5. Elutsükli valitsemine

Kõikides identiteedi elutsükli faasides tuleb identiteediga seonduvaid transaktsioone juhtida kõikehõlmava ja põhjaliku poliitika alusel ning korrastada neid ülevaatlikul moel. See tähendab seda, et on paika pandud täpsed ja konkreetsed (miks ka mitte automatiseeritud)

[18] ingl. *deprovisioning*

reeglid ja juhised, mismoodi erinevatel identiteedi elutsükli astmetel tuleb tegutseda. Identiteediga seonduvate protsesside juhtimine on oluline osa organisatsiooni siseelust ning seetõttu on vajalik üldine kooskõlas protsesside juhtimine. Identiteedihaldusega seonduvaid poliitikaid rakendatakse autentimisel ja autoriseerimisel. Autentimispoliitikad määratlevad identiteedi usaldusväärsuse taseme vastava transaktsiooni lõikes. Autoriseerimispoliitikad määratlevad subjektile kehtivad tingimused, mille alusel võimaldatakse subjektile ligipääs teenustele või ressurssidele. Subjektidel, identiteeti pakkuvatel ja identiteeti kasutavatel osapooltel võivad olla erinevad poliitikad. Näiteks määratlevad nad subjektid, asukohad (kust ligipääsud tehakse) ja ligipääsude ajad. Identiteedipoliitika on lai mõiste, mis ei hõlma ainult valitsemist, vaid mida kasutatakse ka muudel eesmärkidel, näiteks määrates privaatsus-poliitikaid kasutajate ja teenusepakkujate vahel. Kogu identiteedi elutsükli jooksul tuleb tagada ka tegevuste auditeeritavus läbi logimise. (Bertino & Takahashi, 2011)

Kokkuvõtvalt võib öelda, et digitaalse identiteedi elutsüklil on mitmed tähtsad ülesanded – usalduse saavutamine ja säilitamine ning informatsiooni jagamine erinevate osapoolte vahel, mis teevad identiteedi elutsükli korraldamise üsna keeruliseks tehniliseks ettevõtmiseks. Keerukust suurendab ka identiteetide arv ning osapoolte paljusus.

1.3. Identifitseerimine ja autentimine

Autentimine on elektroonilistes keskkondades väga olulisel kohal. Ligipääs ressursile saab aga alguse identifitseerimisprotsessist. Autentimine koosneb identifitseerimisest ja tegelikust autentimisest. Protsessi, mille käigus subjekt väidab end olevat teatud identiteet, näiteks edastab süsteemile kasutajanime, nimetatakse identifitseerimiseks[19] (isikusamasuse tuvastamine ehk tõendamine, siin ja edaspidi identifitseerimine). Protsessi, mille käigus subjekt lisaks kasutajanimele lisab ka korrektse parooli, nimetatakse autentimiseks[20]. Kogu selle protsessi eesmärgiks on tagada ainult volitatud subjektidele ligipääs arvutisüsteemile, võrgule või konkreetsele teenusele. Subjektid on määratletud identiteetidega autentimissüsteemis ning iga identiteet on omakorda seostatud autentimiseks vajalike mandaatidega, mis on teada ainult subjektile ning mida saab süsteemi abil kontrollida. Eeldus, et subjekt hoiab talle väljastatud mandaati saladuses, välja arvatud ettenähtud arvutisüsteemiga mandaadi jagamisel, tagab subjekti identiteedi autentsuse. (Benantar, 2006) Lühidalt on identifitseerimine mittesalajase

[19] ingl. *identification*

[20] ingl. *authentication*

informatsiooni edastamine, mis ütleb, et tegemist on kasutajaga. Autentimine on aga protsess kus tõestatakse identifitseerimise käigus edastatud tunnuste õigsust või kuuluvust. Soovitud identifitseerimisastme tagamiseks kasutatakse kolme tüüpi autentimisviise:

1. Ühe teguriga – esitades midagi, mida kasutaja teab. See võib olla näiteks ema neiupõlve nimi või kooli nimetus. Tavaliselt kasutavad telekomid ja abiliinid[21] seda autentimismeetodit. Ka parooli või PIN-koodi kasutamine kuulub siia kategooriasse.
2. Kahe teguriga ehk kaksikautentimine – esitades midagi, mis kasutajal on. Lisaks sellele, et kasutaja teab midagi, eeldab kahe teguriga autentimine, et kasutaja esitab midagi. Näiteks ID-kaart, kus lisaks PIN-koodile peab kasutajal olema ka kaart kaardilugejas.
3. Kolme teguriga – esitades midagi, mida kasutaja on. Lisaks sellele, et kasutaja teab midagi ning kasutajal on midagi, peab kasutaja ka „olema midagi“. Kolmandaks teguriks on tavaliselt biomeetrilised (eristatava püsitunnuse) tuvastusvahendid, nagu näiteks sõrmejälg, silma vikerkesta skaneerimine, näotuvastus jne. (Williamson, Yip, Sharoni, & Spaulding, 2009) (Benantar, 2006)

Neid kolme autentimisviisi tõlgendatakse erinevates allikates erinevalt, näiteks eeltoodust erinev ja autori arvates korrektsem tõlgendus on selline, et on olemas kolm eraldiseisvat autentimise tegurit:

1. „midagi teadma“
2. „midagi omama“
3. „midagi olema“

Kui on esindatud kasvõi üks neist teguritest, on tegemist ühe teguriga autentimisviisiga. Kui on esindatud kaks tegurit kolmest, on tegemist kaksikautentimisega ning kõigi kolme esinemisel on tegemist kolmikautentimisega. Ehk kui on esindatud näiteks parool („midagi teadma“) ja sõrmejälg („midagi olema“), on tegemist kaksikautentimisega. (Wikipedia.org, Two-factor authentication, 2011)

Need kolm meetodit on põhimõtteliselt teineteisest erinevad. Biomeetrilisel lähenemisel pole mingisugust seost paroolide või füüsilise objektiga, nagu näiteks ID-kaart ja sõrmejälje skanner. Samuti on täiesti erinevad usalduse saavutamise elemendid. Paroolid toetuvad salastatud informatsioonile, samas füüsilised objektid toetuvad sellele, et objekt on turvalises

[21] ingl. *help desk*

kohas ning valvatud. Biomeetria aga tugineb inimese bioloogilisele unikaalsusele. Olenemata millist autentimismeetodit kasutatakse, vajab kaugelt autentimine[22] turvalist andmevahetus-kanalit. Selleks kasutatakse informatsiooni krüpteerimist ja lahenduseks on näiteks otspunkt-krüpteerimine[23]. Et vältida infopüüki[24] igal tasemel, peab suhtlus toimuma osapoolte vahel üle krüpteeritud kanali. Internetiühendus, mis ühendab kliendi mingi veebiteenusega, näiteks veebiserver või vaheserver[25], võib jätta maha andmeid, mis on avatud infopüügile. Otspunktkrüpteerimise puudumisel muutub parooli moodustamise tehnika kõige haavatavamaks ja kõige lihtsamaks murdekohaks[26]. Kui parooli edastatakse avatekstina[27], peab ründaja parooli teadasaamiseks ainult ühendust pealt kuulama. Samamoodi alluvad ka biomeetrilised autentimisviisid rünnetele. Sellised lekked võivad toimuda pikaajaliselt ning märkamatult, põhjustades suurt kahju. (Benantar, 2006)

Käesolevas peatükis anti ülevaade digitaalsest identiteedist ning sellega seonduvatest protsessidest. Kokkuvõttena võib öelda, et digitaalne identiteet on abstraktne ning laialivalguv mõiste, kuigi protsessid, mis seonduvad digitaalse identiteediga on loogilised ja iseenesest-mõistetavad. Digitaalne identiteet annab võimaluse pääsuõiguste loomiseks elektroonilistes keskkondades ning seda tutvustabki järgmine peatükk.

[22] ingl. *remote authentication*

[23] ingl. *end-to-end encryption*

[24] ingl. *interception*

[25] ingl. *proxy server*

[26] ingl. *breach*

[27] ingl. *cleartext*

2. PÄÄSUÕIGUSED

Eelmises peatükis selgitati digitaalse identiteedi mõistet, selle elutsüklit ning kirjeldati selle seost identifitseerimise ning autentimise protsessidega. Identifitseerimisele ja autentimisele järgneb tavaliselt autoriseerimine. Sageli on identifitseerimine, autentimine ja autoriseerimine tehniliselt nii tugevalt seotud, et protsessidel ei tehta vahet ja seda mõistetakse kui ühte protsessi. Võib küsida, et miks on vaja detailselt selgitada niivõrd tugevalt seotud protsesse? Vastus on lihtne – tegemist on andmekaitse seisukohalt äärmiselt oluliste protsessidega ning nende mõistmine võimaldab paremini aru saada identiteedi- ja pääsuõiguste halduse temaatikast.

Pääsu reguleerimine[28] ja autoriseerimine[29] või volitamine on sama vanad mõisted kui inimkond ja vara, mida on vaja kaitsta. Vara kaitseks on kasutatud valvureid, väravaid, lukke ja teisi vahendeid, eesmärgiga piirata ligipääsu väärisesemetele. Pääsu reguleerimise vajadus viis ka esimeste turvaliste süsteemide leiutamiseni, näiteks vargakindel kassaaparaat 1879. aastal James Ritty poolt. Tänapäeva IT keskkondades keskendutakse autoriseerimisel sellele, milline kasutaja pääseb arvutisüsteemis asuvale infole ligi või lihtsamalt öelduna „kes saab mida teha“. Pääsu reguleerimine on kõige levinum ja põhimõttelisem turvamehhanism. Võib väita, et pääsu reguleerimisega kohtume igas IT süsteemis ning see kujutab süsteemide arendamisel suurt süsteemiarhitektuurilist ja administratiivset väljakutset. Ärilisest vaatenurgast tähendab pääsu reguleerimine ressurssidele ligipääsu piiramist või lubamist ning ühtlasi ka ärile elutähtsat eelist. (Ferraiolo, Kuhn, & Chandramouli, 2007)

Pääsu reguleerimine keskendub volitatud kasutajate poolt lubatud tegevustele, vahendades igat subjekti katset pöörduda süsteemis asuva ressursi poole. IT infrastruktuuris võib pääsu reguleerimise süsteeme esineda erinevates kohtades ja erinevatel tasemetel. Operatsioonisüsteemid kasutavad pääsu reguleerimist, et kaitsta faile ja katalooge, kus need asuvad. Andmebaasisüsteemid kasutavad pääsu reguleerimist, et kontrollida ligipääsu andmetabelitele[30] ja andmevaadetele[31]. Enamus kommertssüsteeme ja – rakendusi sisaldavad pääsu reguleerimise vahendeid, mis on tihtipeale sõltumatud operatsioonisüsteemist või andme-

[28] ingl. *access control*

[29] ingl. *authorization*

[30] ingl. *table*

[31] ingl. *view*

baasisüsteemist, kuhu need paigaldatakse. Pääsu reguleerimise eesmärgiks märgitakse tihti süsteemsete ressursside kaitset ebasobivate või ebasoovitavate subjektide eest. Ärilisest vaatenurgast vaadatuna võiks selline eesmärk olla sõnastatud ka kui „optimaalne info jagamine“, kuna infotehnoloogia põhieesmärgiks on informatsiooni kättesaadavaks tegemine kasutajatele ja rakendustele. Võib väita, et mida suurem on jagatud informatsioon, seda suurem on ka tootlikkus. Kuigi pealtnäha segavad pääsu reguleerimise süsteemid info jagamist, siis tegelikkuses toetab hästi korraldatud ja hallatud pääsu reguleerimise süsteem info jagamist. (Ferraiolo, Kuhn, & Chandramouli, 2007)

2.1. Autoriseerimine

Autoriseerimine on protsess, kus otsustatakse, kas juba identifitseeritud ja autenditud subjektil on lubatud pääseda ligi ressurssidele. Autoriseerimine eest vastutab tihti ligipääsu pakkuv teenus. Näiteks kui subjekt soovib ligi pääseda failile, mis asub failiserveril, siis on see failiteenuse kohustus määratleda, kas antud subjekt pääseb failile ligi või mitte. Autoriseerimine võib olla mitmekülgne ja võib teha vahet sellistel tegevustel, nagu lugemine, kirjutamine, kustutamine, käivitamine jne. Enne kui autoriseerimine saab aset leida, peab subjekt olema identifitseeritud ja autenditud. Autoriseerimine toetub identifitseerimis-informatsioonile, et tagada pääsuloend[32] iga teenuse jaoks. Operatsioonisüsteemid aitavad tüüpiliselt autoriseerimisele kaasa, pakkudes rakendustele autoriseerimise vahendeid. Samas on ka paljudel rakendustel omad autoriseerimise mudelid ja vahendid. Subjekt võib olla autenditud, kasutades kindlat identiteeti, kuid ta võib taotleda autoriseeringut ligipääsuks ressursile teise identiteedi alt. Kui subjekt taotleb sellist ligipääsu, siis sellist lähenemisviisi kutsutakse autoriseerimisidentiteediks[33]. Kui see teostatakse rakenduse või teenuse poolt, siis seda kutsutakse kehastumiseks[34]. Kehastumise puhul võib subjekt omada autentimisprotsessi poolt autenditud identiteeti. Lisaks sellele võib subjekt ajutiselt või pidevalt kasutada identiteedi autoriseeringut kui kasutaja on autoriseeritud operatsioonisüsteemi või rakenduse poolt, et kehastuda teiseks identiteediks. Kehastumise protsess on väga otstarbekas ja kasulik klient-server süsteemides, kus serveril töötav rakendus toimib serveri õigustes, pääsedes ligi kasutajale vajalikele ressurssidele, et neid kasutajale edastada. Kehastumine võimaldab

[32] ingl. *access control list*

[33] ingl. *authorization identity*

[34] ingl. *impersonation*

subjektil ühenduda serverile kasutades kellegi teise laiemaid või kitsamaid pääsuõigusi. (Todorov, 2007)

Autentimine ja autoriseerimine toimivad käsikäes ja tihti on raske tõmmata joont, kus lõpeb autentimine ja algab autoriseerimine. Teoorias peab autentimine tuvastama ainult subjekti identiteedi, autoriseerimine aga on vastutav selle eest, et määratleda, kas subjekt peaks saama ressurssidele ligi või mitte. Et luua arusaadav ja loogiline seos nende kahe protsessi vahel, on operatsioonisüsteemides ja rakendustes kasutusel sisselogimisprotsess[35]. Sisselogimisprotsess pakub kasutaja identifitseerimist - ta algatab autentimisdialoogi kasutaja ja süsteemi vahel ning tekitab kasutajale operatsioonisüsteemi või rakendusse spetsiifilise struktuuri, mida nimetatakse pääsuvahendiks[36]. See pääsuvahend lisatakse igale protsessile, mille kasutaja käivitab. Seda kasutatakse autoriseerimisprotsessis, et teha kindlaks, kas subjektile on lubatud ligipääs või mitte. Pääsuvahendi struktuur on lüliks autentimise ja autoriseerimise vahel. Pääsuvahend sisaldab kasutaja autoriseerimisega seonduvat informatsiooni, kuid see informatsioon saadakse tavaliselt subjekti identifitseerimise ja autentimise protsessis. Sisselogimisprotsess võib samuti täita turvalisusega mitteseonduvaid ülesandeid. Näiteks võib see protsess seadistada kasutaja töökeskkonda lisades spetsiaalseid seadeid töökeskkonda sisselogimisel. (Todorov, 2007)

2.2. Pääsuõiguste poliitikad

Üks maailma esimesi organisatsioone, kes püüdis süstematiseerida pääsu reguleerimist ja pääsuõigusi oli Ühendriikide Kaitseministeerium[37]. 1983. aastal anti Ühendriikide Kaitseministeeriumi poolt välja dokument nimega «Trusted Computer System Evaluation Criteria» (TCSEC), mille sisuks oli antud organisatsioonis rakendatavate pääsu reguleerimise viiside kirjeldamine. Kirjeldati mandatoorset (MAC)[38] ja diskretsionaarset (DAC)[39] poliitikat. Pääsuõigused jaotatakse tihti diskretsionaarseteks ning mittediskretsionaarseteks. Diskretsionaarseks pääsupoliitikaks on DAC ja mittediskretsionaarseteks on MAC ning rollipõhine

[35] ingl. *user logon process*

[36] ingl. *access token (mitte segamini ajada identity token ehk identsustõend)*

[37] ingl. *Department of Defence*

[38] ingl. *mandatory policy*

[39] ingl. *discretionary policy*

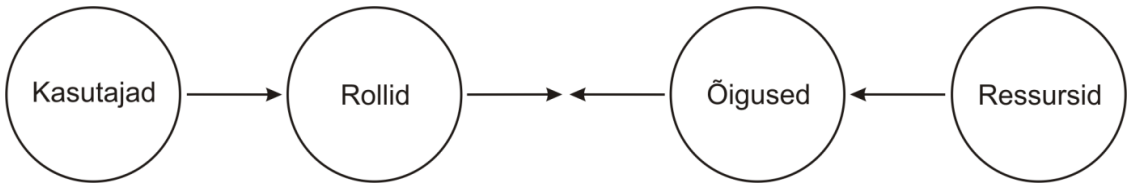
pääsupoliitika (RBAC)[40]. (Wikipedia.org, Access control, 2011) Benantar Messaud jagab oma raamatus pääsuõiguste poliitikad või paradigmad aga kolmeks:

- diskretsionaarsed (DAC);
- mandatoorsed (MAC);
- rollipõhised (RBAC). (Benantar, 2006)

Mandatoorse pääsupoliitika puhul on omanik või omaniku esindaja see, kes määrab pääsuõiguste poliitika ning peakasutajad ja kasutajad on kohustatud seda poliitikat järgima. Diskretsionaarse poliitika puhul jäetakse peakasutaja otsustada, millistele kasutajatele millised ligipääsuõigused väljastatakse. Niipea kui kasutajale antakse ligipääs, muutub kasutaja peakasutajaks, kuna kasutajal on õigus anda teistele kasutajatele õigusi. (Department of Defence, 1985) Nii mandatoorse kui ka diskretsionaarse poliitika puhul on leitud täiendava uurimistöö ja praktika käigus, et need pealtnäha turvalised poliitikad võivad pika kasutamise tagajärjel luua kontrollimatu ja andmelekkeks sobiva pinnase. (Windley, 2005) Samas on aga DAC maailmas kõige laiemalt levinud ja omaks võetud pääsupoliitika, kuna see sobib hästi kokku päris-elu protsessidega. Ühtlasi on viimastel aastatel aina rohkem levinud rollipõhine pääsupoliitika, milles sisaldub teatud määral diskretsionaarse pääsupoliitika komponente ning mis teoorias sobib kokku nii DAC kui MAC mudelitega. (Benantar, 2006)

2.2.1. Rollipõhise pääsukontrolli poliitika

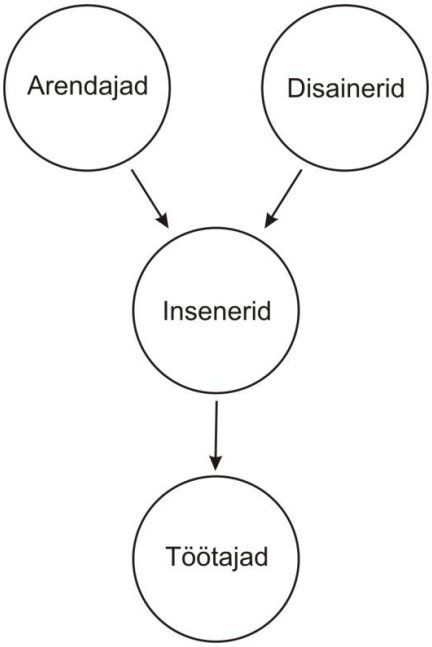
Rollipõhine pääsupoliitika RBAC on muutunud aktuaalseks MAC ja DAC alternatiiviks. RBAC reguleerib pääsu ressurssidele, süsteemidele ja äriprotsessidele vastavalt subjekti rollile. Roll on abstraktsioon, mis sisaldab endas teatud vastutust ja kohustusi koos lubatud tegevuste kogumiga. Erinevalt diskretsionaarsest ja mandatoorsest pääsupoliitikast antakse rollipõhise pääsuõiguste poliitika puhul õigused rollidele, mitte subjektidele. (Benantar, 2006) Rollipõhist pääsuõiguste poliitikat iseloomustab alljärgnev joonis 3:



Joonis 3. Rollipõhise pääsuõiguste poliitika joonis. (Windley, 2005)

[40] ingl. *role-based access control*

Rollipõhise pääsupoliitika oluliseks tunnuseks on see, et kogu ligipääs on korraldatud läbi rollide. Teine oluline tunnusjoon rollipõhise pääsuõiguste poliitika puhul on see, et rollid võivad olla hierarhilise iseloomuga. Hierarhiat iseloomustab joonis 4:



Joonis 4. RBAC hierarhia. (Windley, 2005)

Kui rollid luuakse antud joonise järgi, siis niipea kui töötajale määratakse rolliks disainer, on ta automaatselt ka inseneride osakonna liige ning töötaja ning talle kehtivad osakonna ja töötajate rollid. Lisaks sellele, et rollid võivad olla hierarhilise iseloomuga, saab rollidele määrata parameetreid, mis aitavad rolle hallata. Rollipõhised autoriseerimisskeemid põhinevad kolmel reeglil:

1. Rolli määramine - kõikidele süsteemi subjektidele on määratud rollid, rollideta subjektid ei saa süsteemis midagi teha.
2. Rolli autentimine - enne kui subjektile omistatakse roll, peab subjekt olema autenditud.
3. Tegevuste autoriseerimine - subjekt saab teostada tegevusi ainult siis, kui see tegevus on autoriseeritud subjekti osas kehtiva rolli jaoks.

Rollipõhine autoriseerimine on paindlikum kui autoriseerimisskeem, mis põhineb lihtsatel gruppidel ning turvalisem kui selles skeemis, kus kasutajad autoriseeritakse grupist sõltumatult. Veelgi enam, praktika näitab, et rollipõhise autoriseerimisskeemi puhul on lihtne lisada, eemaldada ja piirata subjektide ligipääse ressurssidele kui subjekti ülesanded organisatsioonis muutuvad, isegi siis kui need muutuvad igapäevaselt. (Windley, 2005)

3. IDENTITEEDIHALDUS

Identiteedi mõistet iseloomustab hästi illustratsioon, kus üks koer ütleb teisele: *„Internetis ei tea keegi, et sa oled koer“*. (Reed, 2002) Identiteedihaldusel on kirju minevik. Ajalooliselt on erinevad kogukonnad identiteedihaldusele lähenenud erinevatest vaatenurkadest lähtuvalt. Mõned kogukonnad on rahul sellega, et valitsus jälgib üksikisikute identiteete, mõned aga mitte. Näiteks Teise maailmasõja ajal pidid kodanikud kaasas kandma dokumente, et vajadusel oma kodakondsust tõestada. Mitmetes Aasia riikides on indiviidid kohustatud kaasas kandma isikut tõendavaid dokumente, et vajadusel riigivõimu esindajatele oma isikut tõendada. Isikute jälgimist ja dokumentide kaasas kandmist peetakse üldiselt politseiriigi tunnuseks ja seda üritatakse igal juhul vältida. Näiteks 1987. aastal lükkasid austraallased jõuliselt tagasi eelnõu, millega taheti kehtestada riiklik ID-kaart, mille eesmärgiks oli riigi poolt pakutavate teenuste parem haldamine. Tulemusena ei koondatud isikuandmeid ühte andmehoidlasse ja riigi võimalused kodanikke jälgida ahenesid. Negatiivne on aga see, et pettused, mida pannakse korda riigi teenuste osas, õitsevad. Riigiasutuste tasemel kehtib sama olukord. Isikuga seonduvad andmed asuvad laiali erinevates andmehoidlates ning puudub võimalus neid andmeid ühendada, et luua täielik pilt isikuandmetest ja pääsuõigustest. Selline olukord on tõsiselt segavaks asjaoluks asutuste võimekusele hakkama saada järjest suurenevate riigi või ettevõtluskeskkonna poolt tulenevate nõuetega. (Williamson, Yip, Sharoni, & Spaulding, 2009)

Identiteedihalduse mõiste on tekkinud üsna hiljuti, alles 21. sajandi alguses. Ühtlasi on IH mõiste tõstatanud palju vaidlusi, kuna tegemist on abstraktsiooniga. IH olemus lahendusena seisneb selles, et pakkuda protsesside ja tehnoloogiate kombinatsiooni, tagamaks ja kindlustamaks turvaline ligipääs ettevõtte informatsioonile ja ressurssidele, samaaegselt kaitstes kasutajate andmeid. IH võib tagada võimekuse efektiivselt hallata sisemisi ja väliseid protsesse organisatsioonis, töötajate; klientide; partnerite ning isegi rakenduste jaoks, põhimõtteliselt kõigile või kõigele, mis vajab ettevõttega suhtlust. (Reed, 2002) IH on lahti mõtestatud mitut moodi. Hurwitz Group ütleb 2001. aasta raportis, et IH fookuseks on kasutajaõiguste haldus – kasutajakontode loomine, haldamine, kustutamine ning IH toetab autentimist ja pääsuõigusi. Giga Information Group ütles 2002. aastal, et IH hõlmab endas integratsioonitooteid, näiteks ettevõtte kataloog, ainulogimine[41] ja kasutajakontode haldus;

[41] ingl. *single sign-on*

moodustades ühtse raami, mille ülesandeks on hallata kasutajate infot ja pääsuõigusi üle erinevate süsteemide. Ettevõtete huvi IH vastu suureneb pidevalt, mitte ainult seetõttu, et IH suurendab turvalisust, vaid ka seetõttu, et IH tegeleb kulude ohjamisega, nagu süsteemide kasutajate produktiivsus, IT halduse efektiivsus, helpdeski kulude vähendamine, rakenduste arendamise kiirus ning turvaauditid ja turvapoliitikate vastavuse tagamine. (Reed, 2002)

Võib öelda, et IH on organisatsiooni töötajatele, inimestele ja ettevõtetele omaste andmete, ruumi ja nende jagamise organiseerimine. Inimesed ja ettevõtted võivad olla nii sisemised kui välimised, nii kliendid kui tarnijad. (Williamson, Yip, Sharoni, & Spaulding, 2009) Veelgi üldistades on IH lai valdkond, mis tegeleb isikute identifitseerimisega süsteemis, milleks võib olla riik, arvutisüsteem, arvutivõrk või organisatsioon ja kontrollib pääsu ressurssidele selles süsteemis, kehtestades piirangud subjektide identiteetidele. (Wikipedia.org, Identity management, 2011)

IH on tugevalt seotud mitmete erinevate aspektidega – tehniline aspekt (identiteedihalduse süsteemid), õiguslik aspekt (andmeturbe korralduslikud küsimused), sotsiaalne aspekt (privaatsuse küsimused) ja organisatsiooniline aspekt (ligipääsude hierarhiad). Maailma-vaateliselt on identiteedihaldust ka jaotatud kolmeks:

1. Puhta identiteedi paradigma - identiteetide loomine, haldamine ja kustutamine, pääsuõigused sealjuures pole olulised.
2. Pääsu paradigma - lähtepunktiks on kasutajale ligipääsu tagamine, kasutaja identiteetide sidumine erinevates infosüsteemide ja rakendustes.
3. Teenuse paradigma - lähtepunktiks on kõik organisatsiooni poolt väljapoole pakutavad teenused. (Wikipedia.org, Identity management, 2011)

Kui varem vaadeldi pääsuõigusi kasutaja vaatenurgast lähtuvalt ning pääsuõiguste alustalaks olid lihtsad kirjutamise ja lugemise õigused, siis tehnoloogia arenguga on olukord muutunud selliselt, et lihtsad lugemise ja kirjutamisega seonduvad õigused pole enam piisavad ning vaja on rohkem informatsiooni selleks, et pääsuõiguseid realiseerida. See informatsioon on aga hulk atribuute, mis loovad subjekti digitaalse identiteedi. Digitaalse identiteediga seonduvat on vaja korraldada ning protsesse on vaja juhtida. Kui digitaalset identiteeti ümbritsevaid protsesse on palju ning need on omavahel seotud, on mõistlik välja töötada lahendus, mis lihtsustab nende protsesside juhtimist. Selleks ongi välja töötatud identiteedihaldussüsteemid, millest räägitakse järgnevas jaotises.

3.1. Identiteedihaldussüsteemid

Töö alguses tutvustati identiteedi mõistet, selgitati identifitseerimist, autentimist ning autoriseerimist ning peatüki alguses selgitati identiteedihalduse olemust. Kõiki neid, eelnevalt selgitatud ning kirjeldatud teemasid ja protsesse võtab kokku mõiste identiteedihaldus ja tehniliselt realiseerivad seda identiteedihaldussüsteemid[42] (edaspidi IHS).

Inimene suudab meeles pidada mõningaid detaile teistest inimestest, kuid suurtes organisatsioonides, kus on näiteks tuhandeid töötajaid, pole kõiki inimesi võimalik meeles pidada. Selliste probleemide ületamiseks on loodud identiteedihaldussüsteemid. IHS võimaldab luua selget ja unikaalset identiteeti igale subjektile ning olemile, lihtsustada ja selgitada iga identiteediga seonduvat konteksti ning määratleda turvapoliitikaid vastavalt profiilidele. Erinevad identiteedihaldust toetavad tehnilised lahendused pakuvad tavaliselt lihtsakoelist lahendust, et saada ülevaade identiteetide kasvust ning keerukusest ettevõttes, tagavad ühetaolise konfiguratsiooni erinevates infosüsteemides, kus kasutajaid luuakse, kustutatakse või muudetakse mingil moel. IHS ühendab omavahel autentimise, autoriseerimise ja pääsuõigused üle erinevate iseseisvate infosüsteemide, nagu näiteks Oracle andmebaas, Microsoft Active Directory jne. IHS ülesandeks on efektiivselt hallata lõplikku subjekti identiteeti, tagades, et kasutajatel on kiire, usaldusväärne ja turvaline ligipääs informatsioonile, infosüsteemidele ja rakendustele. IHS hõlmab nelja protsessi (inglise keeles nelja A'd):

- autentimine (*authentication*) – kasutaja tõendamine;
- autoriseerimine (*authorization*) – kasutaja pääsuõiguste määratlemine;
- pääsukontroll (*access control*) – pääsuviiside haldamine;
- auditeerimine (*audit*) – raporteerimine ja auditeerimise kontrollimine.

Valdavalt arvatakse, et efektiivse identiteedihalduse taga peab olema üks keskne identiteedihaldussüsteem või andmehoidla. Tegelikkuses ei pea see nii olema, kuigi selline lähenemine vähendab kindlasti tehnilist keerukust ja lihtsustab haldamist. (Reed, 2002)

Keskne IHS tagab ülevaatlikkuse, kontrollitavuse ning tervikluse, samas loob keskselt kontrollitav IH lahendus ka potentsiaalse ründeobjekti, mistõttu pole selline ülesehitus otstarbekas, vaid turvalisem on kasutada hajussüsteeme.

[42] ingl *identity management systems (IMS)*

Digitaalse identiteedi haldamiseks on loodud palju erinevaid tehnilisi lahendusi – identiteedihaldussüsteeme. Identiteedihaldussüsteemid on FIDIS (Future of Identity in the Information Society) poolt liigitatud kolmeks:

1. Identiteedihaldussüsteemid kontohalduseks.
2. Identiteedihaldussüsteemid kasutajainfo isikustamiseks[43].
3. Identiteedihaldussüsteemid kasutaja poolt kontrollitud ja hallatud kontekstipõhiseks rolli- ja pseudonüümide halduseks. (Structured Overview on Prototypes and Concepts of Identity Management Systems, 2005)

Tüüpiline IHS sisaldab kasutaja iseteeninduskeskkonda, parooli algseadistust, paroolide haldust, töövoogusid, identiteetide ja ressurssidele ligipääsu andmist ja võtmist.

IHS põhilisteks tegevusaladeks on määratleda subjekti või olemi identiteet; hoida asjakohast informatsiooni subjektide ja olemite kohta (näiteks nimed ja tõendid) turvalises, paindlikus ja kohandatavas keskkonnas; teha eelpoolnimetatud informatsioon kättesaadavaks standardsete protseduuride või liideste abil; pakkuda paindlikku, hajutatud ja võimsat infrastruktuuri identiteedihaldusele ning aidata hallata ressursside- ja olemitevahelisi seoseid. Messaoud Benantar määratleb raamatus «Access Control Systems» neli identiteedihalduse mudelit:

1. Lokaalse identiteedi mudel[44].
2. Võrguidentiteedi mudel[45].
3. Föderatiivse identiteedi mudel[46].
4. Globaalse veebiidentiteedi mudel[47]. (Benantar, 2006)

3.2. Lokaalse identiteedi mudel

Lokaalse identiteedi mudel on pärit arvutisüsteemide algusajastust, kus arvutamine oli ühe süsteemi keskne. Peremeessüsteem peab lokaalse identiteedi mudeli puhul lokaalset registrit identiteetidest ehk kasutajatest. Kasutajad ja muud süsteemi kasutavad subjektid on kõik tuvastatavad läbi identiteetide, mis on süsteemis olemas. Väline subjekt, kes soovib süsteemi kasutada, peab hankima omale süsteemi kasutamiseks identiteedi. Uus identiteet peab olema

[43] ingl. *profiling*

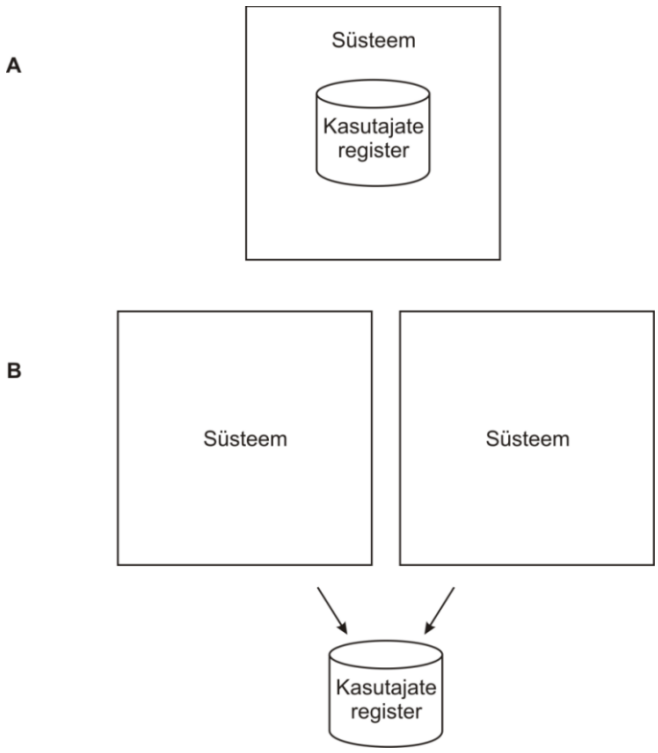
[44] ingl. *local identity*

[45] ingl. *network identity*

[46] ingl. *federated identity*

[47] ingl. *global web identity*

kooskõlas lokaalse süsteemi nõuetega ning olema unikaalne võttes arvesse juba registris olemasolevaid kasutajaid. Kasutajate lisamine ja/või eemaldamine ei mõjuta teisi kasutajaid. Hallatakse õigusi, mis on seotud ainult konkreetse lokaalse süsteemi ressurssidega. Selline mudel tagab lihtsuse, kuid komistuskivideks on süsteemi mahuga seonduvad küsimused ning lame nimemudel[48] ehk nimede ühesuse probleem, mis võib tekkida kui ettevõttes on samanimelised kasutajad. Süsteemi liigsel koormamisel kasutajate ja subjektide informatsiooniga võivad tekkida jõudlusprobleemid ning lame nimemudel ei võimalda süsteemset kasutajate ja subjektide haldust. Lokaalse identiteedi mudelit kirjeldab alljärgnev kaheosaline joonis 5:



Joonis 5. Lokaalse identiteedi mudelid. (Benantar, 2006)

Joonisel kujutatud variandi A puhul on lokaalsel süsteemil kasutusel eraldiseisev kasutajate register, samas variandi B puhul on register jagatud mitmete lokaalsete süsteemide vahel. Kasutajate registri jagamisega võib leevendada süsteemikeskset identiteedihaldust selliselt, et kasutaja registreeritakse ainult ühe korra ja seda registreeringut jagatakse erinevate lokaalsete süsteemide vahel.

Lokaalse identiteedi mudeli eeliseks on selle lihtsus, kuid on ka mitmeid puudusi, nagu eelpool nimetatud käideldavuse ja nimede ühesuse probleem. Käideldavus jaguneb jõudluseks

[48] ingl. *flat namespace*

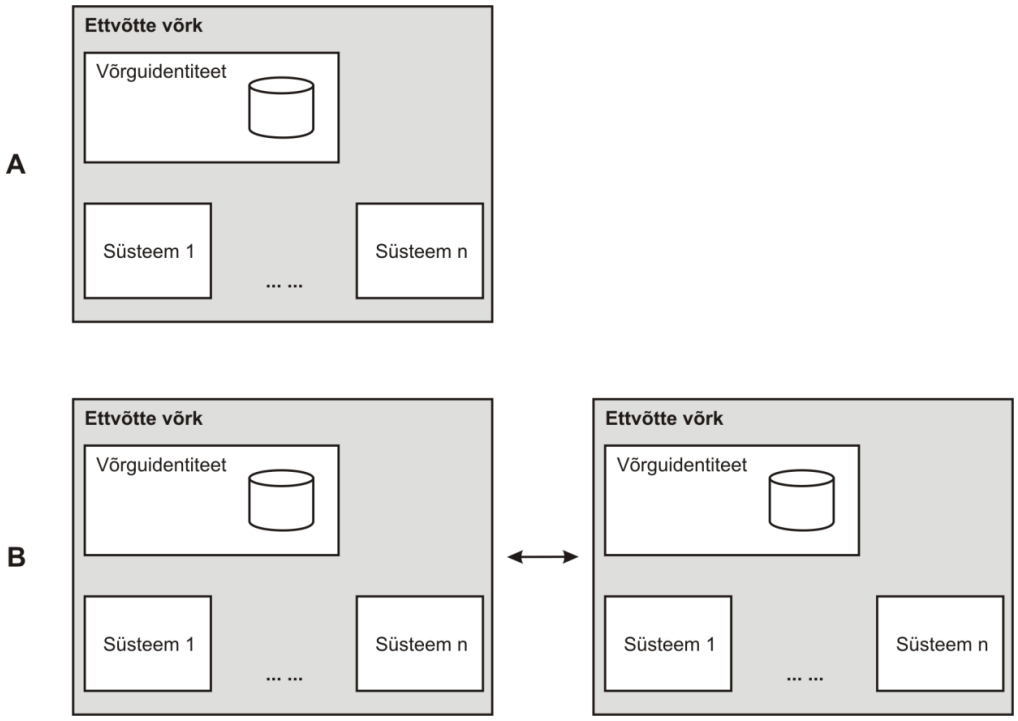
ja mahtuvuseks ning lokaalse identiteedi mudeli puhul võivad mõlemad saada komistuskivideks. Süsteemi haldamine võib lokaalse identiteedi mudeli puhul olla samuti raskendatud kui kasutajaid ja süsteemi kasutavaid ressursse on palju, kuid sellele on olemas lahendused, näiteks parooli sünkroniseerimine[49], mis erineb ainulogimisest. Üheks paroolide sünkroniseerimise viisiks on ka joonisel näidatud keskne kasutajate register, kuid ka registrite replikeerimine[50] teiste lokaalsete süsteemide vahel. (Benantar, 2006)

3.3. Võrguidentiteedi mudel

Hajussüsteemide levik oli põhjuseks, miks tekkis võrguidentiteedi mudel. Idee ise on lihtne, kuid laiahaardeline - identiteet on autenditud arvutisüsteemide võrgus, kuid mitte ainult ühe süsteemi suhtes. Kui identiteet on tuvastatud, siis võib see identiteet navigeerida läbi võrgu, kasutades teenuseid ja pääsedes ligi ressurssidele, ilma et subjekt peaks otseselt uuesti oma identiteeti tõendama. Selle mudeli puhul pole identiteet enam ühes süsteemis, vaid ühes võrgus, mille raames see identiteet ka kehtib. Et saavutada võrguidentiteedi mudel, on vaja, et identiteediteenused oleksid võimalikud kõigi võrgus olevate süsteemide puhul. Selle mudeli puhul on raamideks tavaliselt üks ettevõte, kuigi süsteemide võimekus lubaks ka mitmete ettevõtete vahelist identiteedihaldust, ehk mitmete võrguidentiteetide sidumist, näiteks domeenidevahelise Kerberose (arvutivõrgu autentimisprotokoll) rakendamist – näiteks Microsoft Active Directory'te sidumine. Võrguidentiteedi mudelit iseloomustab alljärgnev kaheosaline joonis 6:

[49] ingl. *password synchronization*

[50] ingl. *replication*



Joonis 6. Võrguidentiteedi mudel. (Benantar, 2006)

A puhul on identiteet piiratud ühe ettevõtte võrguga, B puhul on identiteet jagatud kahe ettevõtte võrgu vahel. Põhiline erinevus lokaalse mudeli jagatud registri ja võrguidentiteedi mudeli vahel seisneb kasutuse laiuses - jagatud registri kasutamine on võimalik ainult üksikute süsteemide lõikes, võrguidentiteedi kasutamine on võimalik väga erinevate rakenduste, süsteemide ja seadmete lõikes. (Benantar, 2006)

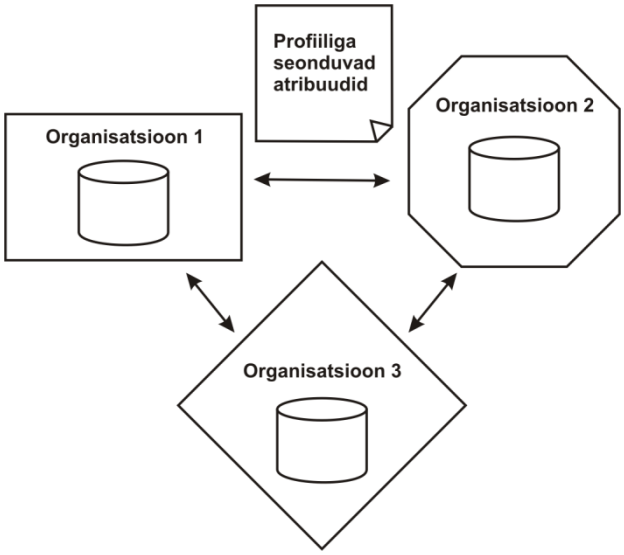
3.4. Föderatiivse identiteedi mudel

Mõiste föderatsioon on abstraktne ning seda tõlgendatakse erinevates allikates mitmetähenduslikult. Föderatsiooni mõiste annab tunnetuslikult edasi paindlikkuse mõtte ning tekitab tunde mitmetest erinevatest subjektidest, mis teevad koostööd. Interneti nimeteenuse (DNS)[51] puhul viitab föderatsioon volituste delegeerimisele (domeenide delegeerimine) nimeserverite vahel. Elektroonilises maailmas võib föderatsioon tähendada erinevate ettevõtete infrastruktuuride vahelist suhet või seost. Identiteedi tasemel avaldub föderatsioon läbi selliste lahenduste, kus üks organisatsioon võimaldab otseteenuseid või ressursse teise organisatsiooni registreeritud subjektidele föderatsiooni või liidestuse või kokkuleppe raames. Tulemuseks on olukord, kus föderatsiooni liikmed on saavutanud identiteediruumi laienemise

[51] ingl. *domain name services*

väljapoole ettevõtet, ilma et ettevõte peaks haldama lisandunud identiteetide kogumit. Föderatiivse identiteedi mudeli alustalaks on ettevõtetevaheline usaldus[52]. Föderatsioon saavutatakse läbi selliste vahendite, mis võimaldavad hankida usaldusväärset informatsiooni väliste identiteetide kohta, mis soovivad süsteemile ligi pääseda. Usaldusväärne informatsioon väliste identiteetide kohta saadakse enda ettevõtte seest turvalisel viisil. Selline protsess saavutatakse kasutajatele ja süsteemidele läbipaistvalt, ehk siis lõppkasutaja ei taju sellist ettevõtetevahelist infovahetust. Lõppkasutaja ei pea end teise ettevõtte juures registreerima ega autentima. Föderatsiooni abil vahetatakse ettevõtete vahel subjektide atribuute kokkulepitud kujul ja viisil. Föderatsiooni loomise kõige suuremaks tehniliseks komistuskiviks ongi atribuutide vahetamise viis ning süntaks[53]. (Benantar, 2006) Selle probleemi lahenduseks on välja töötatud XML keelel põhinev vabavaraline standard SAML (Security Assertion Markup Language). (OASIS, 2011)

Föderatiivse identiteedi mudelit iseloomustab joonis 7:



Joonis 7. Föderatiivse identiteedi mudel. (Benantar, 2006)

Joonisel on näha erinevad organisatsioonid erinevate kujunditena, mis iseloomustab asjaolu, et erinevad organisatsioonid haldavad enda identiteedi mudelit, mis võib olla sama, mis teistes organisatsioonides, mis kuuluvad antud föderatsiooni. Organisatsioone ühendavad nooled iseloomustavad usaldussuhteid, mis on turvaliselt kontrollitavad.

[52] ingl. *trust*

[53] ingl. *syntax*

3.5. Globaalse veebiidentiteedi mudel

Vajadus globaalse veebiidentiteedi mudeli järele tekkis tänu veebi arengule tõsiseltvõetavaks infotöötlusplatvormiks. Veebiidentiteet on identiteet, mida tuntakse üle kogu veebi. Analoogiliselt veebis asuvatele ressurssidele, millel on oma universaalne ressursiidentifikaator (URI)[54], esineb ka veebiidentiteet globaalses interneti kontekstis. Iga veebiidentiteet esindab kindlat olemit, kes seda identiteeti omab, samamoodi, nagu URI esindab kindlat ressurssi, mis URI taga on. Erinevalt aga URIdest, mis esindab ressursse ja mis on asutuse poolt hallatavad, on veebiidentiteeti võimalik tuvastada ja kasutada mitmetes erinevates veebisüsteemides, kaasa arvatud lokaalsetes süsteemides. Selleks, et tehniliselt realiseerida globaalset veebiidentiteedi mudelit, on vaja identiteedid siduda erinevate identiteediregistritega, kus antud identiteet eksisteerib. Kui selline lahendus on loodud, siis on võimalik sujuvalt ja lõppkasutajale läbipaistvalt navigeerida läbi erinevate veebis asuvate teenuste ja ressursside. Selliseid tehnilisi lahendusi on tänapäeval mitmeid, nende hulka kuuluvad ka metakataloogid[55] ja virtuaalkataloogid[56]. (Benantar, 2006)

3.6. Metakataloogid

Hierarhilisi andmebaase kutsutakse kataloogideks[57]. Kataloogid on mõeldud organisatsiooni struktuuri säilitamiseks, on optimeeritud identiteetide ja sellega seonduvate andmete säilitamiseks ning kiireks leidmiseks. Metakataloogi on nimetatud Burton Group poolt 1996. aastal kui „kõikide kataloogide ühendkataloog“. (Goldsmith & Mulqueen, 1999) Metakataloogid on üheks IHS osaks ning üks digitaalse identiteedi loomise (provisjoneerimise) ja tühistamise (deprovisjoneerimise) tehniliseks lahenduseks. Metakataloogi all mõistetakse lahendust, mis koosneb teistes kataloogides asuvast informatsioonist, käesoleval juhul identiteedist ja tema atribuutide kogumist. Üldiste atribuutide haldamine käib metakataloogi kaudu ning atribuudid sünkroniseeritakse automaatselt teistesse kataloogidesse laiali. Allolev joonis 8 iseloomustab metakataloogi.

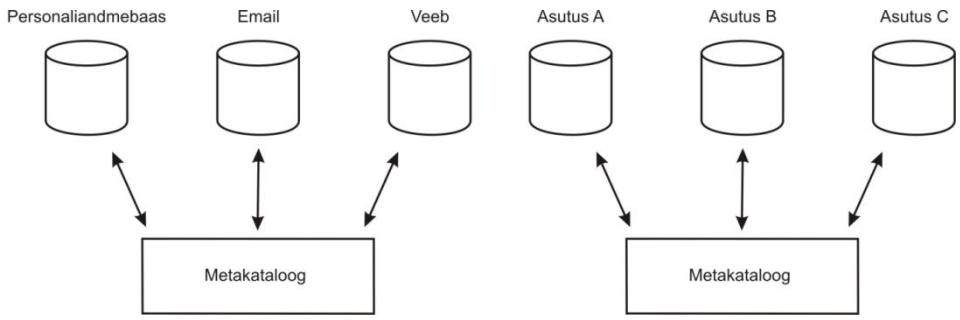
---

[54] ingl. *universal resource identifier*

[55] ingl. *metadirectory*

[56] ingl. *virtual directory*

[57] ingl. *directory*



Joonis 8. Metakataloog. (Benantar, 2006)

Joonis näitab erinevate kataloogide ühendamist ühe metakataloogi abil. Vasakpoolne metakataloog seob mitmed erinevad kataloogid või andmebaasid ühes ettevõttes, parempoolne metakataloog aga seob erinevate ettevõtete kataloogid. Sellise lähenemise nõrgaks küljeks on laiendatavus, kuna kõikide veebiidentiteetide andmebaaside ühendamine on ääretult mahukas. (Benantar, 2006)

3.7. Virtuaalkataloogid

Üheks metakataloogi liigiks on virtuaalkataloogid, mida kutsutakse ka ühendvõrkudeks[58]. Virtuaalkataloogi idee seisneb selles, et ei kasutata täiendavat keskset kataloogi, vaid kasutusel on vahend, mis oskab suhelda kõigi kataloogidega ning mille kaudu on võimalik saada vajalikud atribuudid. (Goldsmith & Mulqueen, 1999) Põhiline erinevus metakataloogi ja virtuaalkataloogi vahel seisneb selles, et viitamine toimub virtuaalkataloogis ilma reaalse andmete liitmiseta[59]. Selline lähenemine tagab parema süsteemi laiendatavuse, sest metakataloogides on identiteetide andmed erinevates kataloogides eraldiseisvalt. (Benantar, 2006)

Eelpool kirjeldatud mudelid on teema mõistmiseks kindlasti vajalikud ning korrastavad abstraktsioone, samas reaalelu süsteemides ei leidu väga palju antud mudelitele täpselt vastavaid süsteeme, vaid leiduvad segamudelid. Raske on ka teoreetiliste mudelite järgi määratleda, milline organisatsioon millist mudelit kasutab. Paljudel organisatsioonidel on kasutusel mitmed erinevad identiteedihalduse süsteemid, mis varieeruvad lokaalsest kuni föderatiivseni, samas on samadel organisatsioonidel identiteediandmebaasid, mis ei ole seotud teiste identiteediandmebaasidega ning identiteedihaldussüsteem võib koosneda nii automaatselt lahendatud protsessidest kui ka käsitsi tehtavatest tegevustest.

---

[58] ingl. *affiliate networks*

[59] ingl. *join*

4. IDENTITEEDI- JA PÄÄSUÕIGUSTE HALDUS EUROOPA LIIDUS

Antud peatükis tutvustatakse tähtsamaid identiteedi- ja pääsuõiguste haldusega seonduvaid projekte ja programme Eestis ja Euroopa Liidus. Eestis on üks põhjapanevamaid riikliku identiteedihalduse alustalasid ID-kaart. ID-kaart ja selle võimalused toetavad ja võimaldavad Eesti osalust Euroopa Liidu erinevates identiteedihalduse programmides ja projektides. Euroopa Liidus algatatud programmid ja projektid on küll tähtsad ja põhjapanevad, kuid need on seotud paljude osapooltega ja seetõttu pole tulemused kiired. EL identiteedihalduse ja infrastruktuuri areng ei toimu ühe-kahe aasta jooksul, vaid tulemusi on oodata ehk ca 5-10 aasta jooksul. Erinevad programmid ja projektid on suunatud erinevate antud valdkonnaga seonduvate teemade uurimiseks ning vahel dubleerivad teineteist. Seetõttu kirjeldab autor antud peatükis tähtsamaid identiteedihaldusega seonduvaid projekte ja programme.

4.1. ID-kaart

Eestis, nagu paljudes teistes Euroopa riikides on isikuttõendava dokumendina kasutusel ID-kaart. Eesti ID-kaardi erinevus teistest seisneb selles, et tegemist on kiipkaardiga, mida saab lisaks tavapärasele isikuandmete ja pildi järgi isiku tuvastamisele, kasutada ka elektroonilises keskkonnas. Elektroonilises keskkonnas saab ID-kaarti kasutada:

- autentimiseks;
- digiallkirjastamiseks;
- krüpteerimiseks;
- identifitseerimiseks - isiku tuvastamiseks elektroonilises keskkonnas.

ID-kaardi puhul on kasutusel kahe teguriga autentimismudel – lisaks kaardi kiibil asuvatele sertifikaatidele, peab kasutaja teadma ka PIN-koode, kusjuures vahet tehakse PIN1 ja PIN2-koodil. PIN1 sisestamist kasutatakse autentimisel ja PIN2 sisestamist allkirjastamisel. ID-kaardi näol on tegemist erasektori ja riigi ühistööna väljatöötatud toetava infrastruktuurikomponendiga, mis lihtsustab kasutaja identifitseerimist ja autentimist ning loob usaldusväärse keskkonna, mida saab rakenduste arendamisel kasutada. ID-kaardi infrastruktuur toetab ka elektrooniliste keskkondade arengut ning on tugev „võimaldaja“ Eesti

infotehnoloogilises arengus. Hea näide on üle-euroopaline elektroonilise identiteedi projekt, mida juhib STORK projekt[60], kus osalemine on Eestil võimalik tänu ID-kaardile.

ID-kaarte antakse välja riiklikult Politsei- ja Piirivalveameti Kodakondsus- ja Migratsiooni-büroo poolt ning ID-kaardi infrastruktuuri haldab AS Sertifitseerimiskeskus.

4.2. STORK

STORK (Secure Identity Across Borders Linked) on konkurentsivõime tõstmise ja innovatsiooni raamprogramm, mis on kaasrahastatud EL poolt. STORK taotleb koostalitlus-võime[61] süsteemi väljatöötamist Euroopa Liidus, mille eesmärgiks on elektroonilise identiteedi (eID) tuvastamise ja autentimise võimaldamine, mis omakorda võimaldab ette-võtlusel, kodanikel ja riigiametnikel kasutada nende riiklikke elektroonilisi identiteete kõikjal EL liikmesriikides. STORK piloteerib ühtlasi ka e-riigi identiteediteenuseid. STORK prog-ramm õpib praktikast, mismoodi selliseid teenuseid arendada ning uurib, millist kasu ja milliseid väljakutseid sellise koostalitlusvõime süsteemi kasutuselevõtt toob. STORK koos-talitlusvõime lahendus elektroonilisele identiteedile toetub hajusarhitektuurile, mis sillutab teed täielikule EL e-teenuste integreerumisele, võttes arvesse spetsifikatsioonid ja infra-struktuuri, mis on liikmesriikides kasutusel. Lahendus, mida välja töötatakse peaks olema elujõuline, läbipaistev, turvaline kasutada ja mastabeeruv[62] ning peab olema rakendatud sellisel viisil, et lahendus on jätkusuutlik ning on pikema elueaga kui piloot ise. STORK projekt:

- arendab ühtsed reeglid ja spetsifikatsioonid et toetada ühist elektroonilise identiteedi tuvastamist üle riigipiiride;
- katsetab toimivates keskkondades turvalisi ja lihtsalt kasutatavaid elektroonilise identiteedi lahendusi kodanike ja ettevõtete jaoks;
- teeb koostööd teiste EL algatustega, et maksimeerida elektroonilise identiteediteenuse kasulikkust. (European eID Interoperability Platform , 2009)

Eestit esindab STORK programmis AS Sertifitseerimiskeskus ning üks esimesi piloote on tehtud Eesti Infotehnoloogia Sihtasutuse (EITSA) hallatava SAISga (Sisseastumise infosüsteem) 2010. aastal, kus SAIS liidestati STORK projekti raames väljatöötatud Pan-

[60] ingl. *Secure Identity Accross Borders Linked*

[61] ingl. *interoperability*

[62] ingl. *scalable*

European Proxy Services (PEPS) lahendusega ning selle abil saavad SAISi kasutada Eesti ülikoolidesse sisseastujad teistest riikidest, näiteks Itaalia, Saksamaa, Rootsi jne.

4.3. FIDIS - Future of Identity in the Information Society

FIDIS näol on tegemist Euroopa Komisjoni poolt algatatud 6. raamprogrammi ühe instrumendi, Network of Excellence (NoE) põhjal algatatud projektiga, mille eesmärgiks on arendada infoühiskonda. EIS (European Information Society) digitaalne tegevuskava ütleb: „Digitaalse tegevuskava üldine eesmärk on tagada jätkusuutlik majanduslik ja sotsiaalne kasu, mida annab kiirele ja ülikiirele internetiühendusele ja koostalitlusvõimelistele rakendustele tuginev digitaalne ühtne turg.“

FIDIS tegeleb tehnoloogiaga, mille eesmärgiks on usaldus ja turvalisus ning ühtlasi isikute privaatsuse säilitamine.

FIDIS on jaotatud seitsmeks uurimisvaldkonnaks:

1. „Identiteedi identiteet[63]“.
2. Profileerimine.
3. Identiteetide koosvõime ja identiteedihaldussüsteemid.
4. Privaatsus ja identiteedi õiguslik-sotsiaalne sisu.
5. Kõrgtehnoloogiline identiteet.
6. Mobiilsus ja identiteet. (Future of Identity in the Information Society (FIDIS), 2004)

[63] ingl. *identity of identity*

5. UURING

Eelnevates peatükkides kirjeldati identiteedi- ja pääsuõiguste halduse teoreetilist osa – tutvustati digitaalse identiteedi mõistet, selle elutsüklit, avati identifitseerimise, autentimise, autoriseerimise mõisted ning räägiti pääsuõiguste poliitikatest. Selgitati identiteedihalduse süsteeme ja identiteetide mudeleid, tutvustati suuremaid identiteedi- ja pääsuõiguste haldamisega seonduvaid projekte Eestis ja Euroopa Liidus. Teoreetilise osa kirjeldamine toob käsitletavasse teemasse selguse ja võimaldab teadlikult ja selge fookusega läbi viia töös püstitatud hüpoteeside uurimise.

Käesolevas peatükis tutvustatakse uurismetoodikat, uuringu planeerimist, uuringu jaoks välja töötatud raammudeleid, uuringu läbiviimist ning uuringus osalenud asutusi ja infosüsteeme.

5.1. Uurimismetoodika ja uuringu planeerimine

Identiteedi- ja pääsuõiguste halduse temaatika uurimiseks avalikus sektoris, viidi läbi juhtumiuuringud. IPH terminoloogia ei ole eesti keeles väga hästi arenenud ja üks-üheselt mõistetav. Ühtlasi on IPH teema tundliku iseloomuga, sest riigiasutuste infosüsteemid sisaldavad delikaatseid isikuandmeid, maksusaladust, riigisaladust jms. Seetõttu polnud võimalik andmete kogumiseks kasutada küsimustikku, vaid kasutati intervjuud. Lisaks intervjuudele töötati läbi internetis ja avalikes andmekogudes leiduv informatsioon. Avaliku sektori asutused on kohustatud avalikustama peetavate andmekogude kohta informatsiooni Riigi Infosüsteemi Haldussüsteemis (RIHA), seetõttu oli RIHA oluliseks infoallikaks. Intervjuude tarbeks tuli luua küsimustikud, kuid selleks, et küsimustega saavutada võimalikult täpne eesmärk, tuli luua raammudelid, mis aitaksid täpsustada uuritavat eesmärki ning korrastada kogutavat andmestikku. Raammudelite abil selgusid IPH temaatika mõõtmed ning mudelite analüüsimisel otsustati uuringus keskenduda organisatsiooni ja infosüsteemi tasemetele. Organisatsiooni ja infosüsteemi taseme uurimine valiti seetõttu, et need tasemed annavad kõige parema ettekujutuse IPH olukorrast avalikus sektoris ning on operatiivsel tasemel kõige aktuaalsemad. Kuna magistritöö maht on piiratud ning autori käsutuses olevad ressursid samuti, polnud mõeldav läbi viia intervjuusid kõigi avaliku sektori asutustega, vaid tuli valida mõistlik valim. Valimi loomisel töötati läbi RIHAs asuvad materjalid, konsulteeriti spetsialistidega ning kasutati töö autori ning juhendaja kogemusi ning teadmisi. Autor töötab avalikus sektoris ja tal on ülevaade mitmete avaliku sektori asutuste IPH korraldusest. Et teadmistepagasit täiendada ja leida valimisse huvitavaid ja innovaatiliste lahendustega asutusi

ja infosüsteeme, pidas autor nõu IPH temaatika juhtivate arendusspetsialistidega. Valimis keskenduti sellele, et leida huvitavaid ja häid praktikaid, uurida erineva suuruse ja ülesannetega asutusi ja infosüsteeme ning saada selle läbi ülevaade Eesti avaliku sektori IPH korraldusest. On selge, et IPH korraldus on äärmiselt aktuaalne asutustes, kus on palju kasutajaid, suur voolavus või väga olulisel kohal andmekaitse. Selle uurimiseks valiti valimisse nii suure kui ka väikese kasutajate arvuga asutusi ja infosüsteeme. Kuna IPH tehnoloogilise lahenduse ehk identiteedihaldussüsteemi mõiste pole selgepiiriline, siis tuli kvaliteetse võrdlusandmestiku kogumiseks luua raamistik. Peatükis 4 selgitatud identiteedi mudelid kirjeldavad identiteedihalduse teoreetilisi mudeleid, kuid ühtlasi kujutavad ka erinevaid identiteedihaldussüsteeme. Et neid mudeleid uuringu fookuse täpsustamisel aluseks võtta, tuli luua selged piirid kust algab identiteedihaldussüsteem ja kus see lõpeb. Võttes arvesse teoreetilisi identiteedihalduse mudeleid ja reaalset elu, otsustati, et kui organisatsiooni identiteedihalduses esinesid järgmised tunnused, siis oli tegemist identiteedihaldussüsteemiga:

- identiteedi võtmine algallikast on automatiseeritud;
- identiteedi loomine ning kontode sulgemine/peatamine on automatiseeritud;
- digitaalset identiteeti ja tema atribuute hoitakse automaatselt ühetaolisena mitmete ettevõtte jaoks põhiliste või oluliste infosüsteemide lõikes;
- samas kõikides infosüsteemides ja andmekogudes kasutatavad digitaalsed identiteedid ei pea ilmtingimata olema ühendatud.

IHS ei pea tingimata olema keskne lahendus või täielikult automatiseeritud keskkond või keskkonnad. Praktikas võib identiteedihaldussüsteeme kohata ka üleüldise korraldamatuse keskel, kus ümberringi toimub digitaalsete identiteetide elutsükli korraldus käsitsi või üldsegi mitte. Samas arendatakse jõudumööda vanu süsteeme värskele identiteedihaldussüsteemile järele. IPH võib olla vabalt lahendatud käsitööna. Näiteks väiksemas ettevõttes ei ole vajalik ega otstarbekas identiteedi- ja pääsuõiguste haldust automatiseerida. Piisab kui uue töötaja tulles tehakse taotlus ja edastatakse see kooskõlastatult identiteedi loojale, olgu see siis süsteemiadministraator või peakasutaja. Täpselt samadel alustel saab ka identiteedi peatada või konto sulgeda ja identiteedi eemaldada või deaktiveerida. Suuremas organisatsioonis on IPH automatiseerimine oluline, sest suure hulga identiteetide ja pääsuõiguste korrashoid võib olla töömahukas ning vead selles töös võivad luua pinnase turvaintsidentideks. Kuna magistritöös püstitatud hüpoteeside uurimiseks on otstarbekas uurida identiteedihalduse süsteeme, siis on otstarbekas vahet teha automatiseeritud süsteemil ja formaalselt toimival süsteemil. Selline jaotus on uuringus oluline ainult organisatsioonide puhul, kuna seal uuriti

IH olukorda laiemalt. Infosüsteemide tasemel ei ole selline jaotus aktuaalne, kuna seal vaadeldi konkreetseid infosüsteeme, mis ei pruugi olla seotud identiteedihaldussüsteemidega ja on ise identiteedihaldussüsteemid.

Lisaks identiteedihalduse süsteemide tuvastamisele, oli organisatsioonide puhul määravateks asjaoludeks neid süsteeme ümbritsev informatsioon, nagu näiteks kasutajate arv, infosüsteemide ja andmekogude arv, ülesanded jne. Infosüsteemide lõikes keskenduti lahenduse selgitamisele, huvitavate momentide väljatoomisele ning selgitati infosüsteemi kasutamise kasutuslugusid, eesmärgiga leida identiteedi- ja pääsuõiguste halduse parimad praktikad.

5.1.1. Identiteedi- ja pääsuõiguste halduse raammudelid

IPH temaatikat võib vaadelda ja analüüsida mitmeti. Informatsioonist arusaamiseks on vajalik info korrastada ning selleks loodi autori poolt ja juhendaja kaasabil raammudelid. Raammudelite aluseks on vastav kirjandus, kuid valmiskujul neid ei eksisteeri. Näiteks aspektmudeli alged on leitavad Patricia McMillian ja Rodney McDuff esitlusest[64], kus nad kirjeldavad IPH raamistikku Austraalia ja Uus-Meremaa haridusasutustele. Samuti on aspektmudeli alged leitavad Robin McKenzie, Malcolm Crompton ja Colin Wallise artiklist «Use Cases for Identity Management in E-Government»[65].

5.1.1.1. Identiteedi- ja pääsuõiguste hierarhiline mudel

Identiteedi- ja pääsuõigust käsitletakse erinevates allikates erinevate nurkade alt. Levinud lähenemine on selline, kus IPH tutvustamist alustatakse identifitseerimise ja autentimisega ning lõpetatakse identiteeti puudutavaga. Sellise ülesehitusega on näiteks raamatud «Access Control Systems - Security, Identity Management and Trust Models» (Benantar, 2006) ja «Digital Identity» (Windley, 2005). Teised allikad keskenduvad identiteedi mõiste selgitamisele ning libisevad identifitseerimise, autentimise, autoriseerimise, auditeerimise ning pääsuõiguste poliitika mõistetest sujuvalt üle, neid sügavuti käsitlemata. Messaoud Benantar on raamatus «Access Control Systems» öelnud, et turvaline identifitseerimine on tänapäeva andmeturbe nurgakiviks. See aga algab kontrollitud identiteedi loomisega. Et

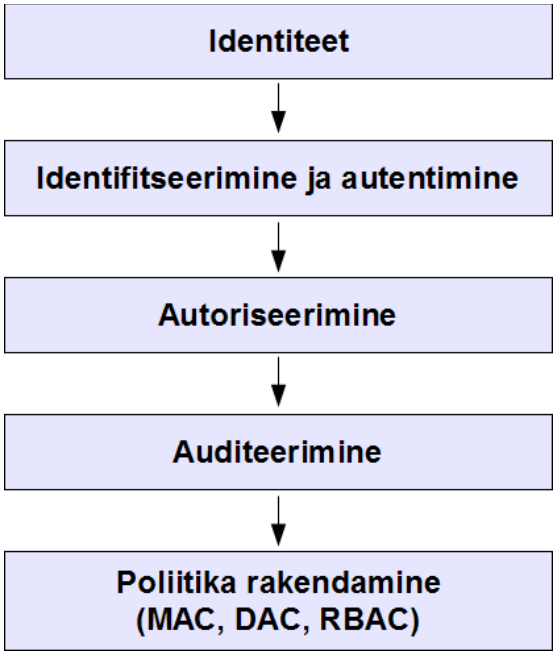
---

64 http://www.caudit.edu.au/educauseaustralasia09/assets/presentations/wednesday/Patricia%20McMillian%20&%20Rodney%20McDuff.pdf

65 http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2008.51

teemat korrastada, pidas töö autor vajalikuks luua hierarhiline mudel selgitamaks identiteedi- ja pääsuõiguste temaatikat üldisemalt.

Joonisel 9 on kujutatud hierarhiline ülesehitus, kus esimesel tasemel on identiteet, mis on kogu identiteedi- ja pääsuhalduse aluseks. Seejärel on võimalik identifitseerimine ja autentimine, mille järel toimub autoriseerimine. Paljudes tänapäeva süsteemides toimub järgmisena auditeerimine, kuigi olenevalt süsteemist võib auditeerimine toimuda ka kõigil eelnevatel ja järgnevatel tasemetel. Kõige lõpuks toimub pääsupoliitika rakendamine. Selline mudel võimaldab paremini mõista identiteedi- ja pääsuõigustega seonduvat ja loob selgust abstraktsesse teemasse.

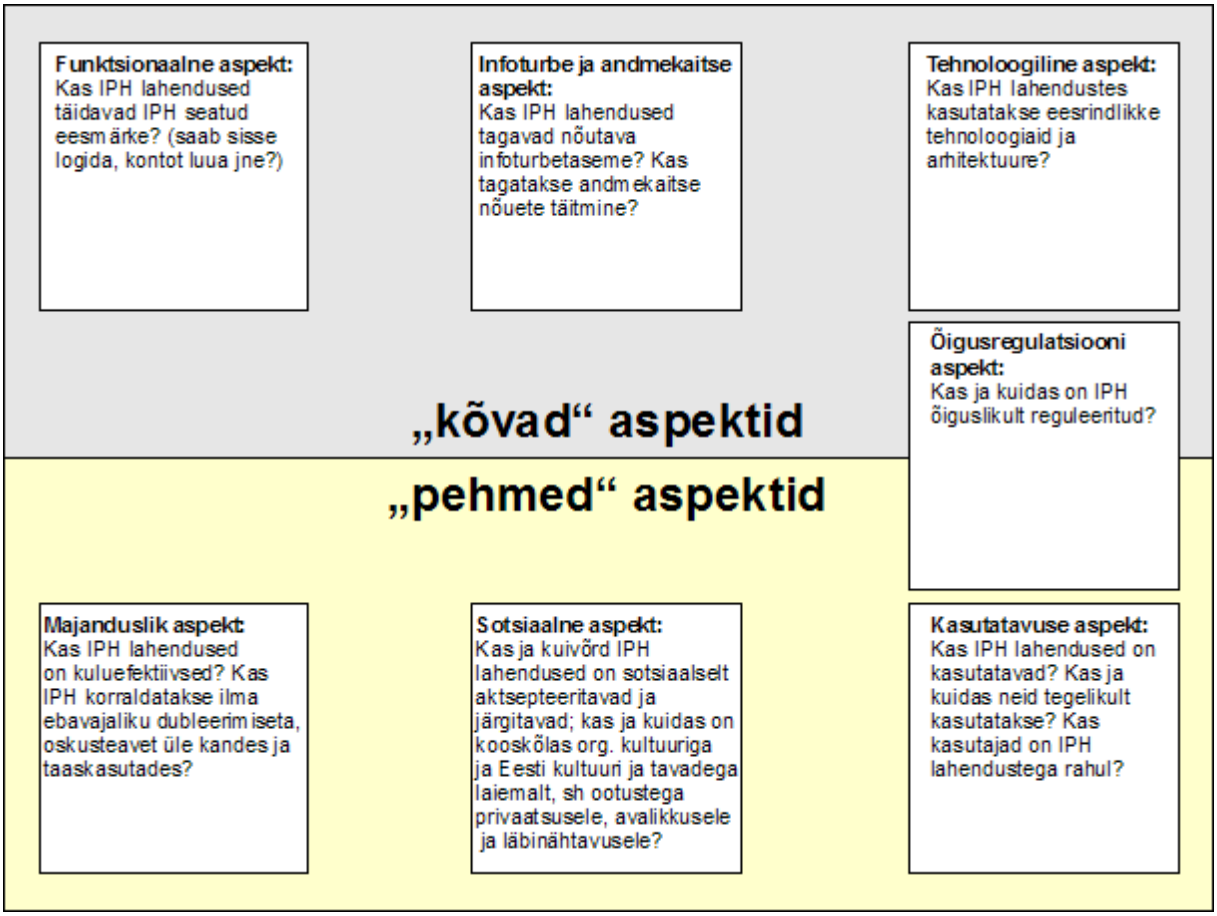


Joonis 9. IPH hierarhiline mudel. (Erend, 2011)

5.1.1.2. Identiteedi- ja pääsuõiguste halduse aspektmudel

Igasugust valdkonda või teemat uurides on otstarbekas välja selgitada vaatenurgad. Kui IPH temaatikat uurida avalikus sektoris, siis on see mitmetahuline ja omab mitmeid vaatenurki, mida muud sektorit uurides ei leia. Avaliku halduse funktsioonid on mitmekesised, erinevates funktsioonides võivad IPH nõuded erineda, näiteks korrakaitse vs haridus. Avaliku sektori organisatsioonid võivad olla suured ja haralised, suur tähtsus on kultuuril ja tavadel, kodaniku usaldusel riigi vastu ning suurt rolli mängib ka riigi üldine poliitiline süsteem. (Parmakson, 2011) Vaatenurkade korrastamiseks töötati magistritöö juhendaja Priit Parmaksoniga koostöös poolt välja aspektmudel, mida kujutab joonis 10. Joonisel jagatakse vaatenurgad

kaheks – nn „kõvad“ aspektid ja „pehmed“ aspektid. Kõvade aspektide hulka kuuluvad funktsionaalsus, infoturve ning andmekaitse ja tehnoloogia. Õiguslik aspekt positsioneerub nende vahele, kuna osaliselt on regulatsioonid olemas, osaliselt tuleb need asutusepõhiselt välja töötada. Pehmete aspektide hulka kuuluvad majanduslik aspekt, kasutatavus ning sotsiaalne aspekt.



Joonis 10. IPH aspektmudel. (Parmakson, 2011)

5.1.1.3. Identiteedi- ja pääsuõiguste halduse juhtumiuuringute raammudel

Et organiseerida intervjuude käigus kogutavat teavet ning leida täpne fookus, loodi magistritöö juhendaja Priit Parmaksoniga koostöös juhtumiuuringute raammudel (joonis 11). Mudelis eristatakse erinevaid identiteedi- ja pääsuõiguste halduse tasemeid, mis on seostatud erinevate aspektidega. Tasemed muutuvad ülevalt-alla kitsamalt üldisemale ning mudeli järgi saab vaadelda IPH aspekte erinevatelt tasemetelt. See mudel aitab täpsustada ja kitsendada

juhtumiuuringute ringi ning seab piirid uurimisküsimustele. Mudeli analüüsimise tulemusena keskenduti magistritöös infosüsteemi ja organisatsiooni tasemetele ning jagati intervjuude küsimused aspektidesse, nagu näha lisades 1 ja 2.

	F Funktsionaalne aspekt	T Tehniline aspekt	Õ Õigusliku regulatsiooni aspekt	K Kasutatavuse aspekt	M Majanduslik aspekt	S Sotsiaalne aspekt	A Infoturbe ja andmekaitse aspekt
1: Üksikisiku tase							
2: Infosüsteemi mooduli tase							
3: Infosüsteemi tase							
4: Infosüsteemide kogumi tase							
5: Organisatsiooni tase							
6: Riigi tase							
7: Euroopa Liidu tase							

Joonis 11. Juhtumiuuringute raammudel. (Parmakson, 2011)

5.2. Uuringu läbiviimine

Uuringu käigus viidi läbi kahte tüüpi intervjuusid. Ühed, mis käsitlevad identiteedi- ja pääsuõiguste haldust avaliku sektori organisatsioonis ja teised, mis käsitlevad huvitavalt või väljapaistavalt lahendatud identiteetide haldamist infosüsteemi tasandil. Kuna tegemist on erinevate identiteedi- ja pääsuhalduse tasemetega, tuli luua ka mõnevõrra erinevad küsimustikud, mis on näha lisades 1 ja 2.

Juhtumiuuringutes vaadeldi kahte aspekti – organisatsiooniline aspekt ning infosüsteemi aspekt. Infosüsteemide valimisse valiti tehnilised lahendused, mis paistsid millegi poolest silma, eesmärgiga tuvastada parimad praktikad IPH seisukohalt.

Juhtumiuuringud ei ole identiteedi- ja pääsuõiguste tehniliste lahenduste osas väga detailsed, kuna detailsema informatsiooni avaldamine avaliku iseloomuga magistritöös läheks vastuollu asutuste andmekaitse regulatsioonidega. Töö mitteavalikustamine aga ei toetaks magistritöö ühte põhieesmärkidest, milleks on IPH temaatika arendamine. Järgmistes jaotistes tutvustatakse juhtumiuuringus osalenud organisatsioone ja infosüsteeme.

5.2.1. Riigi Infosüsteemide Arenduskeskus

Riigi Infosüsteemide Arenduskeskus (RIA) on Majandus- ja Kommunikatsiooniministeeriumi valitsemisalas tegutsev hallatav riigiasutus, mis osutab avalikke teenuseid ja täidab riiklikke ülesandeid riigi infosüsteemi arendamisel ja haldamisel. Keskuse tegevusvaldkonnaks on riigi

infosüsteemi arendamise ja haldamise korraldamine ning koordineerimine. RIAs on kuus osakonda, kus töötab ligikaudu 60 ametnikku. (Riigi Infosüsteemi Arenduskeskuse põhimäärus, 2009)

Asutust iseloomustavad andmed:

- infosüsteemide kasutajaid u 60;
- andmekogusid ja infosüsteeme u 20;
- identiteet saab alguse mitteautomaatselt personalisüsteemist;
- spetsiaalne identiteedi- ja pääsuõiguste haldussüsteem puudub;
- intervjuu käigus tuvastati, et kasutusel on lokaalse identiteedi mudel.

Intervjuu käigus leitud huvitavad faktid:

- identiteedi- ja pääsuõiguste halduse automatiseerimisele organisatsiooni lõikes suurt tähelepanu ei pöörata, kuna organisatsioon on väike ning automatiseerimisest saavutatav efekt oleks väike;
- organisatsiooni omapära seisneb selles, et see arendab ja haldab riiklikke infosüsteeme ning nendevahelisi seoseid, mistõttu riiklike infosüsteemide osas on identiteedihaldus ja sellega seonduvad tehnilised lahendused väga aktuaalsed.

5.2.2. Põhja-Eesti Regionaalhaigla

SA Põhja-Eesti Regionaalhaigla (PERH) moodustati 25. juulil 2001 Mustamäe haigla, Kivimäe haigla, Eesti Onkoloogiakeskuse, Tallinna Psühhiaatriahaigla, Tallinna Nahahaiguste haigla, Arstliku Perenõuandla ja Kutsehaiguste kliiniku baasil. PERHis töötab enam kui 3400 töötajat. PERH koosneb kaheksast kliinikust - anestesioloogia-, diagnostika-, kirurgia-, psühhiaatria-, sisehaiguste-, onkoloogia- ja hematoloogia- ning järelravi ja hooldus-ravikliinikust. PERHi korpused asuvad Mustamäel, Hiiul, Seewaldis, Pelgulinnas, Kosel ja Keilas.

PERHi tegevusalad:

- osutab ambulatoorset ja statsionaarset eriarstiabi ning kiirabi;
- on tervishoiutöötajate kvalifikatsiooni omandamisele eelneva ja järgneva koolituse õppebaasiks ning viib ka ise läbi tervishoiualast koolitust;
- teeb vajadusel ekspertiise;
- töötab välja, täiustab ja aprobeerib uusi diagnostika- ja ravivõtteid;

- aprobeerib uusi ravimeid ja meditsiiniaparatuuri;
- viib läbi ja osaleb tervishoiualastes uuringutes ning teeb tervishoiualast metoodilist tööd;
- teeb koostööd teiste tervishoiuteenuste osutajatega, erialaühendustega ning muude tervishoiuga tegelevate institutsioonidega;
- tagab osutatavate teenuste kõrgetasemelise kvaliteedi ning vastavuse õigusaktidega esitatavatele nõuetele. (Põhja-Eesti Regionaalhaigla, 2011)

Asutust iseloomustavad andmed:

- infosüsteemide kasutajaid u 2500 (kõik PERHi töötajad pole infosüsteemide kasutajad);
- andmekogusid-infosüsteeme u 50;
- identiteet saab alguse automaatselt personalisüsteemist;
- kasutusel on spetsiaalne IPH süsteem;
- intervjuu käigus tuvastati, et kasutusel on võrguidentiteedi mudel.

Intervjuu käigus leitud huvitavamad faktid:

- autentimine on lahendatud asutusesisese kiipkaardiga;
- kasutusel on kommertstarkvara, mille abil on tänaseks automatiseeritud identiteedi- ja pääsuõiguste haldus kolme põhilise infosüsteemi vahel.

5.2.3. Maksu- ja Tolliamet

Maksu- ja Tolliamet (MTA) on Rahandusministeeriumi valitsemisalasse kuuluv valitsusasutus, millel on juhtimisfunktsioon ja mis teostab riiklikku järelevalvet ning kohaldab riiklikku sundi seaduses ette nähtud alustel ja ulatuses. Amet moodustati 01.01.2004 Maksuameti ja Tolliameti ühendamise teel. MTA tegutseb üle Vabariigi. (Maksu- ja Tolliamet, 2011)

Asutust iseloomustavad andmed:

- infosüsteemide kasutajaid u 1800;
- andmekogusid-infosüsteeme u 240;
- identiteet saab alguse automaatselt personalisüsteemist;
- spetsiaalne identiteedi- ja pääsuõiguste haldussüsteem puudub;
- intervjuu käigus tuvastati, et kasutusel on lokaalse identiteedi mudel.

Huvitavamad faktid:

- MTA haldab paljusid infosüsteeme, mis on seotud Euroopa Liidu liikmesriikide analoogsete infosüsteemidega;
- MTA haldab mitmeid infosüsteeme, mida kasutavad lisaks sisekasutajatele ka väliskasutajad, sh kodanikud;
- e-maksuameti rakendust kasutavad üle poole Eesti Vabariigi kodanikest ja pea kõik juriidilised isikud.

5.2.4. Registrite ja Infosüsteemide Keskus

Registrite ja Infosüsteemide Keskus (RIK) on Justiitsministeeriumi haldusala asutus, mille eesmärgiks on luua integreeritud e-teenuseid pakkuv innovaatiline keskkond riigihaldus-, õigus- ja kriminaalpoliitika efektiivsemaks toimimiseks. RIK moodustati Justiitsministri määrusega 2007. aastal. RIK haldab ja arendab mitmeid riigile ja kodanikule olulisi registreid ja infosüsteeme. Sealhulgas on nii e-Äriregister, e-Notar ja e-Kinnistusraamat kui ka mitmed õigusalased infosüsteemid (kohtute infosüsteem, elektrooniline järelevalve ennetähtaegselt vanglast vabanenutele, kriminaalhooldusregister, riiklik kriminaalmenetlusregister, kinnipeetavate register, e-Toimik, e-Õigus jt). RIKis töötab ligikaudu 150 spetsialisti ning RIK tegeleb ka riiklike projektide teostuse ja juhtimisega. Rahvusvahelises plaanis teeb RIK koostööd erinevate riikide IT asutuste ja struktuuridega.

Asutust iseloomustavad andmed:

- infosüsteemide kasutajaid u 3500;
- andmekogusid-infosüsteeme u 65;
- identiteet saab alguse automaatselt personalisüsteemist;
- spetsiaalne identiteedi- ja pääsuõiguste haldussüsteem puudub;
- intervjuu käigus tuvastati, et kasutusel on lokaalse identiteedi mudel.

Intervjuu käigus leitud huvitavamad faktid:

- RIK haldab mitmeid infosüsteeme, mille kasutajateks on mitmed väliskasutajad, sh ka kodanikud.

5.2.5. Siseministeeriumi Infotehnoloogia- ja Arenduskeskus

Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT) on loodud 2008. aastal. Keskuse tegevusvaldkonnaks on ministeeriumi ja tema valitsemisala sisejulgeoleku tagamiseks vajalike infokommunikatsioonitehnoloogia (IKT) valdkonna teenuste osutamine ja selleks vajalike arendus- ning haldusprotsesside korraldamine ja koordineerimine. SMIT teenindab Siseministeeriumit, Politsei- ja Piirivalveametit, Päästeametit ning Sisekaitseakadeemiat. (Siseministeeriumi Infotehnoloogia- ja Arenduskeskus, 2011)

Asutust iseloomustavad andmed:

- infosüsteemide kasutajaid u 7000;
- andmekogusid-infosüsteeme u 300;
- identiteet saab alguse automaatselt personalisüsteemist;
- kasutusel on spetsiaalne identiteedi- ja pääsuõiguste haldussüsteem;
- intervjuu käigus tuvastati, et kasutusel on võrguidentiteedi mudel.

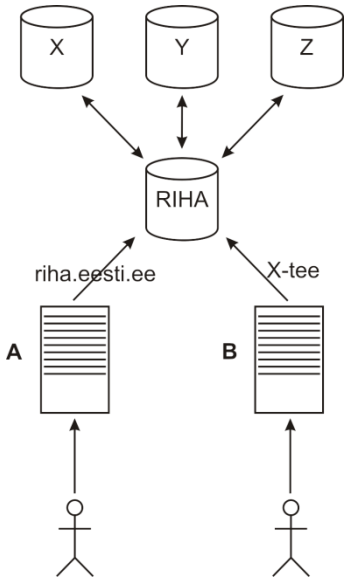
Huvitavamad intervjuu käigus leitud faktid:

- toimib vabavaral põhinev, ise arendatud identiteedi- ja pääsuõiguste halduse süsteem, kuhu on integreeritud mitmed andmekogud ja infosüsteemid ning millega liidestatakse jätkuvalt uusi ja olemasolevaid andmekogusid ja infosüsteeme;
- SMIT on Eesti suurim ja laiahaardelisem avaliku sektori IT kompetentsikeskus.

5.2.6. Riigi infosüsteemi haldussüsteem (RIHA)

Riigi infosüsteemi haldussüsteem (RIHA) on loodud selleks, et kaardistada avaliku sektori, kuid ka erasektori infosüsteemid, andmekogud ja muud komponendid ning pidada nende üle arvestust. RIHAs menetletakse infosüsteemide ja andmekogude asutamist, liitumist X-teega, klassifikaatorite ja XML skeemide haldust ning muid protsesse. RIHA kasutamine on kohustuslik riigi- ja kohaliku omavalitsuse asutustele. RIHA arendab ja hooldab Riigi Infosüsteemide Arenduskeskus.

RIHA puhul on märkimisväärne rakendus ise, mille abil hallatakse teiste infosüsteemide metaandmeid. Ühtlasi on huvitav asjaolu see, et rakenduste haldamisega tegelevate identiteetide ring on suur ning samuti on seoste hulk suur.



Joonis 12. RIHA kasutamise põhimõtteskeem.

Jooniselt 12 on näha, et RIHA on võimalik kasutada üle X-tee (B) või siis veebilehitsejaga (A). X, Y ja Z iseloomustavad erinevaid andmekogusid, kust RIHA identiteetide kohta lisa-informatsiooni (atribuute) ammutab. Nendeks on näiteks Rahvastikuregister, Äriregister, RIA poolt hallatav andmekogu kesksete süsteemide pääsuõiguste haldamiseks jt.

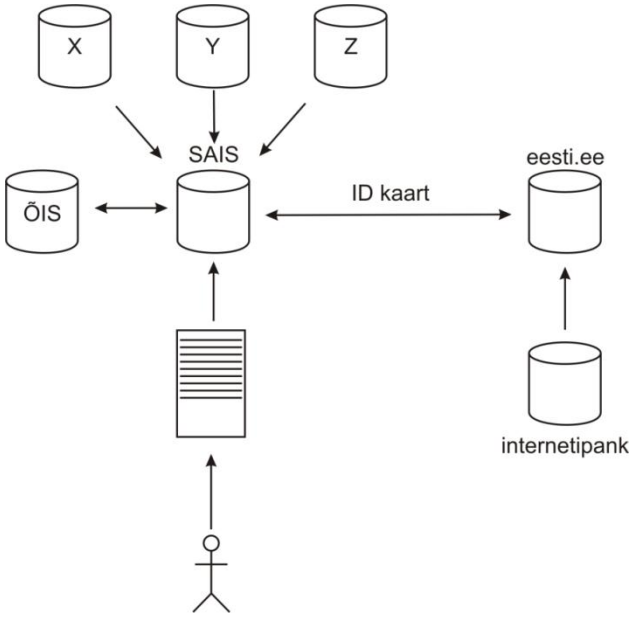
5.2.7. Sisseastumise infosüsteem (SAIS)

Sisseastumise infosüsteem (SAIS) on infosüsteem, mille abil saavad koolide sisseastujad või kandidaadid esitada SAIS-is osalevasse õppeasutusse oma sisseastumisavalduse elektroonselt. Pärast sisseastumisavalduse esitamist aitab SAIS korraldada ka ülejäänud protsessi kuni kooli sissesaamiseni, sh teadete vahendamist sisseastuja ja kooli vahel, õppekoha vastuvõtmist või sellest äraütlemist ja palju muud. SAISi sisselogimine käib ID-kaardi abil. SAIS on seotud teiste riiklike andmekogudega ning andmete olemasolu korral neis pole vaja eraldi tõendada senist haridusteed, riigieksamite hindeid, varasemaid kõrgkooli lõpuhindeid jms. Isegi kui andmeid teistes registrites pole, saab SAIS-is esitada eeltäidetud avalduse vormi, millele tuleb ühes kõrgkoolis lisada tõendus puuduvate andmete õigsuse kohta (nt eelneva kõrghariduse diplom). Ühes õppeasutuses tõenduse esitamisest piisab, kuna kord juba SAIS-i sisestatud ja ühe kooli poolt kinnitatud andmeid on võimalik teistesse õppeasutustesse sisseastumis-avaldust esitades kasutada samaväärselt riiklikest registritest saadud andmetega. SAISi haldab Eesti Infotehnoloogia Sihtasutus (EITSA).

SAIS puhul on märkimisväärne see, et SAIS osaleb STORK projekti piloodis, mille tulemusena välja töötatud Pan-European Proxy Services (PEPS) lahendusega liitunud riikide sisseastu-

jad saavad kasutada SAISi Eesti ülikoolidesse sisseastumiseks. Identiteedi- ja pääsuõiguste mõistes on SAIS huvitav lahendus kahel põhjusel:

1. SAISil puudub autentimismoodul. Autentimiseks kasutatakse www.eesti.ee autentimisvahendeid.
2. SAIS kogub informatsiooni erinevatest andmekogudest, moodustades niimoodi sisseastujate identiteedi.

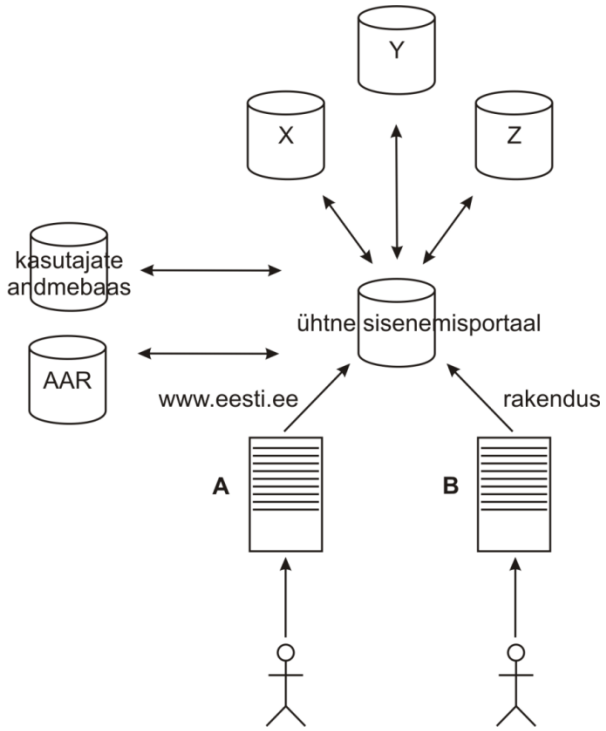


Joonis 13. SAIS sisselogimise põhimõtteskeem.

Põhimõtteskeemilt (joonis 13) on näha, et kasutaja suunatakse SAIS lehelt autentimiseks www.eesti.ee portaali, kus kasutaja autenditakse kas ID kaardiga või läbi internetipanga. Seejärel saab kasutaja kasutada SAIS infosüsteemi. SAIS infosüsteemis annab kasutaja loa pärida tema kohta andmeid teistest infosüsteemidest (X, Y, Z) ning peale nõusolekut moodustatakse kasutajat puudutavatest andmetest identiteet. Peale vastuvõtuperioodi lõppu edastatakse koostatud identiteet haridusasutuste infosüsteemidesse, sh ka ÕISi (Õppeinfosüsteem). SAIS autentimise puhul kasutatakse välist autentimisteenust, mille rakendamisega hoiti kulusid kokku ja taaskasutati olemasolevaid komponente ning selline lähenemine on kindlasti hea praktika nii tarkvaraarenduse kui ka identiteedi- ja pääsuõiguste halduse mõistes. Selliste lahenduste puhul on aga väga oluline teenuslepete olemasolu, millega tagatakse vajalik rakenduse käideldavus.

5.2.8. Ühine sisenemisportaal keskkonnainfo infosüsteemidele

Keskkonnateabe Keskus on Keskkonnaministeeriumi hallatav riigiasutus, mis loodi Keskkonnaministeeriumi Info- ja Tehnokeskuse ning Metsakaitse- ja Metsauuenduskeskuse ümberkorraldamisel. Keskkonnateabe Keskuse tegevusvaldkond on usaldusväärsete ja võrreldavate keskkonnaalaste andmete kogumine, töötlemine, analüüsimine, avalikustamine ning aruandluse esitamine Eesti keskkonnaseisundi ja seda mõjutavate tegurite kohta, samuti asjaomaste andmekogude pidamine. Keskkonnateabe Keskus haldab ca 15 andmekogu ja infosüsteemi, millest enamus on liidestatud keskse sisenemisportaali lahendusega. Alljärgnev joonis 14 iseloomustab keskkonnainfo infosüsteemide ühtse sisenemisportaali kasutamist.



Joonis 14. Keskkonnainfo infosüsteemide ühine sisenemisportaal.

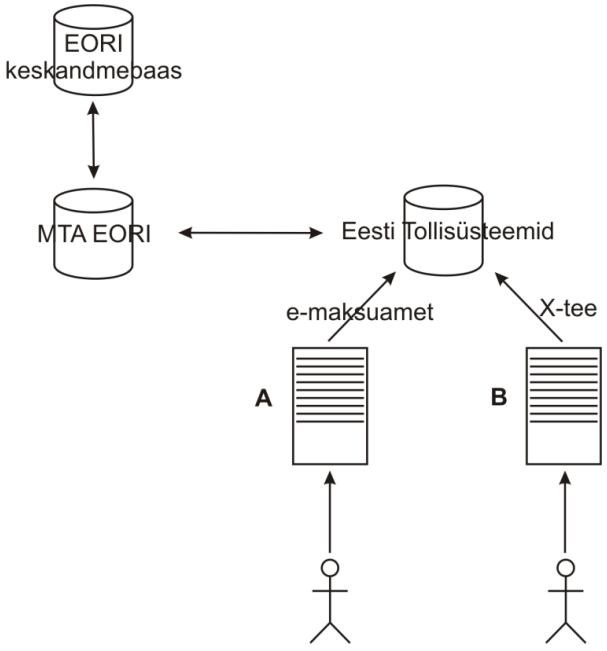
Keskkonnainfo ühtse sisenemisportaali puhul on huvitav asjaolu see, et kasutatakse vabavaralist autentimisteenust pakkuvat lahendust, mis on liidestatud kasutajate andmebaasiga ning RIA poolt hallatava autoriseerimisandmete andmekoguga (AAR), selleks, et kasutajad saaksid autenditud ning autoriseeritud. Kasutusel olev vabavaralise autentimisteenuse serveri puhul on positiivne asjaolu, et selle rakendamise kulud on madalad ning uute rakenduste liidestamine on lihtne, kuna selleks vajalik dokumentatsioon on vabalt kättesaadav ning põhjalik. Vabavaralise ja laialt kasutatava ning arendatava lahenduse eeliseks on arendus- ja ülalhoiukulude kokkuhoid, mis on nii tarkvaraarenduse kui ka identiteedi- ja pääsuõiguste halduse seisukohalt hea praktika.

5.2.9. Ettevõtjate registreerimise ja identifitseerimise süsteem (EORI)

Ettevõtjate registreerimise ja identifitseerimise süsteem (Economic Operators Registration and Identification System) on loodud tollivajadusteks ja on kasutatav Euroopa Liidu tolliterritooriumil kaubavahetuses kolmandate riikidega. Registreerides end ühes liikmesriigis tolliga seotud eesmärkidel, saavad ettevõtjad EORI numbri, mis kehtib terves Euroopa Liidus. Euroopa Liidu tolliterritooriumil asuva ettevõtja registreerib tema asukoha liikmesriigi tolliasutus või EORI numbri väljastamiseks määratud ametiasutus. Ettevõtja, kes ei asu Euroopa Liidu tolliterritooriumil, taotleb EORI numbri talle sobivas liikmesriigis. Eestis omistab EORI numbri Maksu- ja Tolliamet.

Väliskaubandusega tegelevale ettevõtjale omistatakse registreerimisel unikaalne identifitseerimisnumber (EORI number), mis edastatakse EORI keskandmebaasi. Maksu- ja Tolliamet töötas välja rakenduse EORI numbri taotlemiseks Eesti ettevõtjatele ja kolmandate (riigid mis ei kuulu Euroopa Liitu) riikide ettevõtjatele. EORI number omistatakse ettevõtjale üks kord ja selle numbri kasutamisega on ettevõtjal võimalik sooritada tollitoiminguid kogu Euroopa Liidu tolliterritooriumil.

EORIle ligipääsu kirjeldab joonis 15.



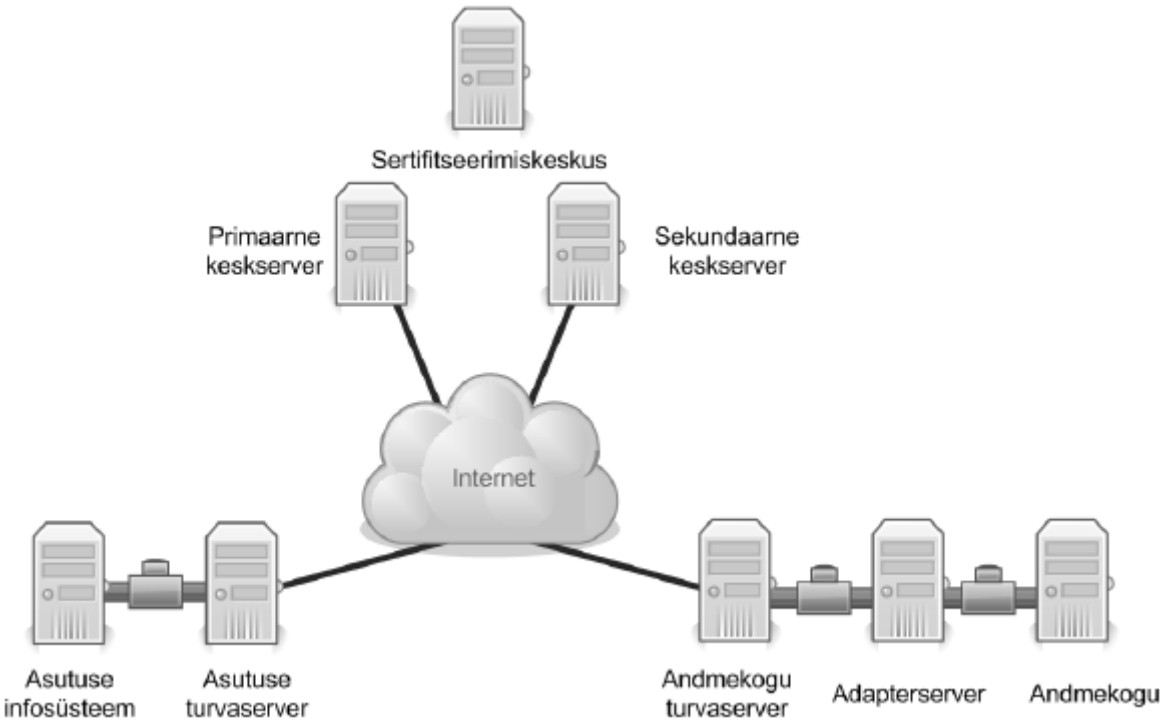
Joonis 15. EORI kasutamine.

Jooniselt on näha, et EORIlt saab kasutada kas läbi e-maksuameti/e-tolli (A) või X-tee kaudu (B).

Maksu- ja Tolliameti poolt välja töötatud EORI rakenduse puhul on märkimisväärne see, kuidas on lahendatud Euroopa Liitu mittekuuluvate riikide tolliettevõtete ligipääs tollisüsteemidele. Selleks, et sellised tolliettevõtted saaksid kasutada Eesti tollisüsteeme, peavad nad omandama EORI numbri, mis tuleb taotleda Eesti Maksu- ja Tolliameti käest, kes peale andmete kogumist edastab need EORI keskandmebaasi ning ühtlasi muutub antud tolliettevõtte esindajaks Eestis, näiteks RIA ees, juhul kui see tolliettevõte soovib X-tee (vajalik vastav sertifikaat) kaudu ühenduda Eesti tollisüsteemidega.

5.2.10. Infosüsteemide andmevahetuskiht (X-tee)

Infosüsteemide andmevahetuskiht (X-tee) on Eesti riigi põhilisi andmebaase ühendav andmevahetuskiht. X-tee võimaldab infosüsteemidel kasutada ühtset juba olemasolevat andmevahetuskeskkonda ja ühte ühtset kasutajaliideste kogumit ning autentimissüsteemi. X-teega liidestamine võimaldab kokku hoida ressursse ning muudab andmevahetuse nii riigiasutuste siseselt kui ka kodaniku ja riigivahelisel suhtlemisel tunduvalt efektiivsemaks. Infosüsteemide andmevahetuskihi rakendamine on kehtestatud Vabariigi Valitsuse 24. aprilli 2008. a määrusega nr 78 "Infosüsteemide andmevahetuskiht". X-tee võimaldab nii kodanikul kui ka ametnikul ja ettevõtjal turvaliselt kasutada üle interneti suurt osa Riigi Infosüsteemi Haldussüsteemis (RIHAs) registreeritud andmebaase. X-tee teenused kodanikule koondavad enda alla erinevad riigi poolt loodud registrid, kus inimene saab teha päringuid ja kontrollida endaga seotud infot. X-tee teenused ettevõtjale annavad ettevõtjatele võimaluse sooritada neid X-tee päringuid, mis on avaliku teenuse kaudu kasutamiseks lubatud. Teenuste kasutamiseks tuleb esmalt ennast ID-kaardi abil või internetipankade kaudu autentida. 31.12.2008 seisuga oli X-teega liitunud üle 100 andmekogu, X-teed kasutas üle 60 000 organisatsiooni. Allolev joonis 16 kujutab X-tee põhikomponente.



Joonis 16. X-tee põhikomponendid. (RIA, 2011)

X-tee puhul on märkimisväärseks asjaolu, et tegemist on riikliku andmevahetust võimaldava lahendusega, kus on edukalt lahendatud identiteedi- ja pääsuõiguste haldus.

6. IDENTITEEDI- JA PÄÄSUÕIGUSED AVALIKUS SEKTORIS

Juhtumiuuringute käigus tuvastati mitmeid mõtteid ja fakte, mida võiks jagada kategooriatesse:

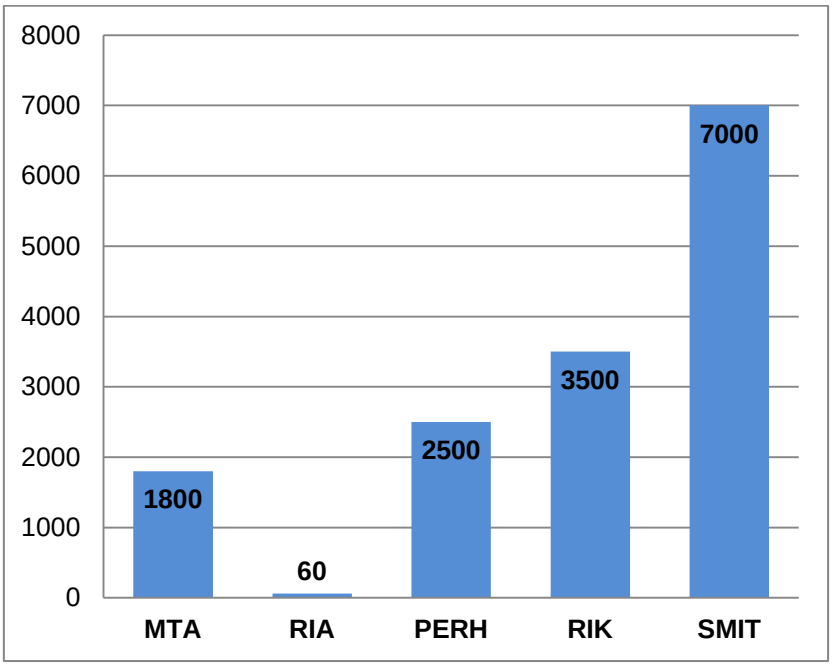
- analoogsete uuringute vajalikkus;
- analoogsete uuringute läbiviimise metoodika;
- IPH süsteemide olukord avalikus sektoris üldiselt;
- parimad praktikad identiteedi- ja pääsuõiguste halduseks.

Kui vaadelda IPH temaatikat kitsalt, siis võiks väita, et on piisav kui asutus korraldab andmekogude ja infosüsteemide identiteedi- ja pääsuõiguste haldust ise, tuginedes mõningatele riiklikele regulatsioonidele, ning täpsem reguleerimine pole vajalik. Kui vaadelda IPH temaatikat üldisemalt, siis näeme, et ühest küljest areneb identiteet ja selle haldus riiklikus ning globaalses suunas. Pole kahtlustki, et need suunad on ühest küljest riikliku infotehnoloogilise innovatsiooni ja arengu võimaldajateks ja teisalt vajalikud, et Eesti Vabariik oleks infotehnoloogiliselt võimekas tegema koostööd teiste riikidega. See on aga võimalik ainult siis, kui kõigi avaliku sektori asutuste poolt suunatakse tähelepanu identiteedihalduse süsteemide täiendamisele ning arendamisele. Intervjuude käigus selgus, et mitmetesse riiklikesse infosüsteemidesse ja andmekogudesse antakse ligipääse kasutajatele väljaspoolt asutust. Väliskasutajateks on tihti teiste riigiasutuste töötajad. Väliskasutajaid haldavad tavaliselt samuti väliskasutajad ja kasutajate haldamine käib käsitsi. See aga tähendab, et inimvea puhul jäävad infosüsteemidesse kasutajad, kes ei peaks seal enam olema, näiteks lõppenud töösuhte tõttu. Selliste kasutajate eemaldamiseks infosüsteemidest häid meetmeid täna pole. Intervjueeritavad on välja pakkunud, et riik võiks välja töötada riigiametnike andmebaasi, mille abil oleks sellised kontrollid võimalikud ja miks mitte automatiseeritud. Intervjuudes selgus ka see asjaolu, et liidestused personaliandmebaasiga selleks, et sealt saada uute või lahkunud kasutajate kohta infot, pole alati olnud lihtsad realiseerida. Mitmel pool riigiasutustes on kasutusel SAP[66] finants- ja personaliinfosüsteem, millega liidestamiseks tuleb läbirääkimisi pidada Rahandusministeeriumiga. IPH temaatikat võiks toetada üleriiklikult, võttes teemaderingi riikliku korraldamise päevakorda. See aga vajab täpsema ja laiema uuringu läbiviimist.

[66] http://www.sap.com/estonia

Uuringute ja erialaseminaris läbi viidud küsimustiku põhjal on selge (21st vastanust teadsid digitaalse identiteedi mõistet ainult 4 ja 10 arvasid, et teavad), et intervjueeritavate jaoks ei ole üheselt selged IPH temaatikaga seonduvad mõisted. Autori kogemus erinevates projektides ja töörühmades ütleb, et see ongi tavaline, et mõistetest saadakse aru erinevalt, kui pole ühtset raammudelit ja definitsioone, millega kõik asjaosalised on tutvunud. Seetõttu on vajalik intervjuudes vältida spetsiifilisi mõisteid, nagu „digitaalne identiteet“, „pääsuõiguste haldus“ jt. Et saada täpsem ülevaade avaliku sektori identiteedi- ja pääsuõiguste halduse korraldusest, on vaja läbi viia täpsem ning suurema valimiga analüüs. Ilmselt ei ole niivõrd mahuka analüüsi raames ratsionaalne andmeid koguda intervjuu abil, vaid otstarbekas on kasutada veebiküsimustikku, kus on ka mõisteid ja IPH temaatikat selgitav osa.

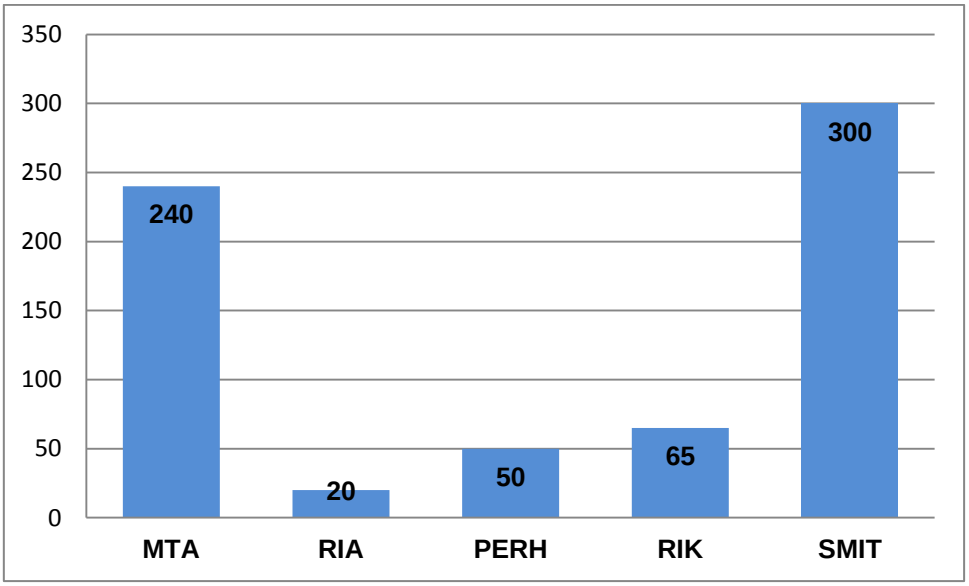
Juhtumiuuringutes erinesid asutused oma tegevusvaldkondadelt ning ülesannetelt. Asutust iseloomustavaks näitajaks on kasutajate arv. Mitmed asutused, nagu näiteks SMIT ja RIK, tegelevad põhitegevusena infotehnoloogiliste teenuste osutamisega, kuid on ka ise enda poolt hallatavate ja arendatavate identiteedi- ja pääsuõiguste süsteemide kasutajad. Kasutajate arv on määravaks teguriks identiteedi- ja pääsuõigustele suunatava tähelepanu ja viimistluse osas. Kasutajate arvu uuringu käigus küsitletud asutustes iseloomustab joonisel 17 kujutatud diagramm.



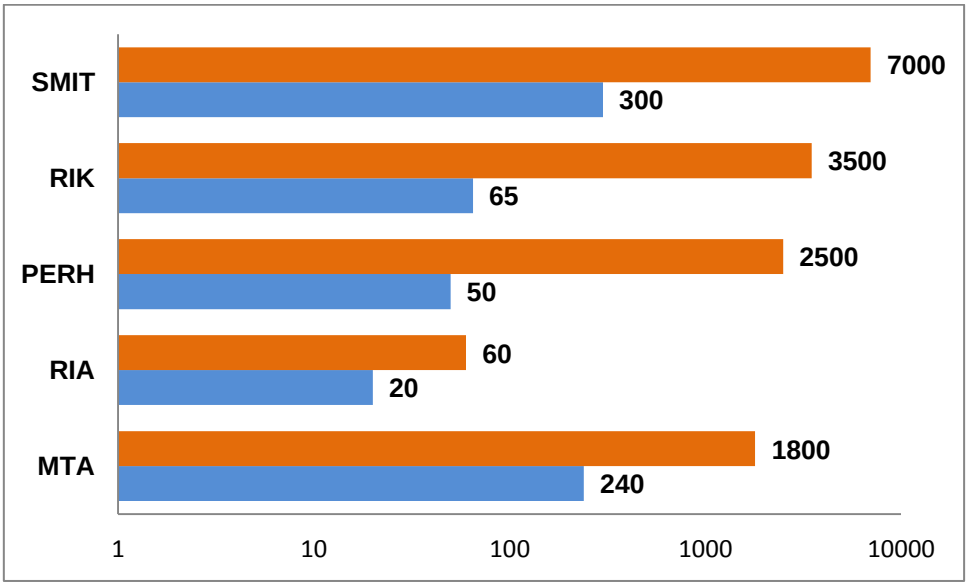
Joonis 17. Kasutajate arv asutuste kaupa.

Teiseks asutusi iseloomustavaks näitajaks on andmekogude ja infosüsteemide arv. Suur andmekogude ja infosüsteemide arv suurendab vajadust identiteetide haldamise järele, nõuab

head autentimise korraldust ning keskselt korraldatud autoriseerimise lahendusi. Vastasel juhul võivad suure tõenäosusega realiseeruda kõrged infoturbega seonduvad riskid. Andmekogude ja infosüsteemide hulka intervjueeritud asutustes iseloomustavad diagrammid joonisel 18 ja 19.



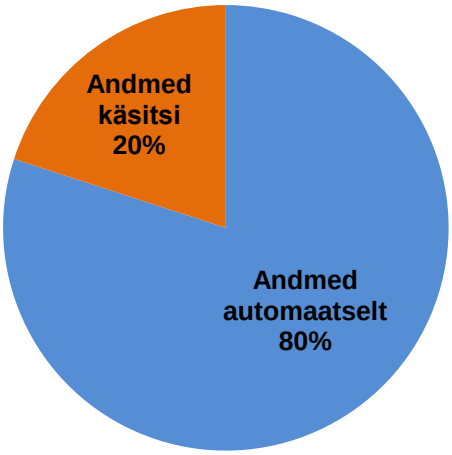
Joonis 18. Andmekogude ja infosüsteemide arv uuringus osalenud asutustes.



Joonis 19. Kasutajate ja infosüsteemide arv uuringus osalenud asutustes.

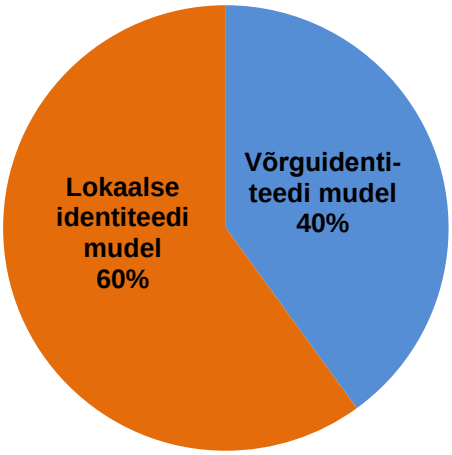
Kirjanduse ja spetsialistide hinnangul on heaks praktikaks digitaalse identiteedi loomine personaliandmebaasist alguse saanud andmete põhjal. Eranditult kõigis uuringus osalenud asutustes saavad digitaalsed identiteedid alguse personaliandmebaasist. Töö esimeses peatükis selgitatakse, et identiteedihaldussüsteemide osaks ja üheks rutiinseks protsessiks on kasutaja-andmete liikumine autentimiskeskkonda ehk identiteedi loomine. Selliste rutiinsete, kuid

andmekaitse seisukohast oluliste tegevuste automatiseerimine on erineva kirjanduse ja eriala spetsialistide hinnangul heaks praktikaks. Joonisel 20 kujutatud diagramm iseloomustab kasutajaandmete autentimiskeskkonda liikumise viise intervjueeritud asutustes.



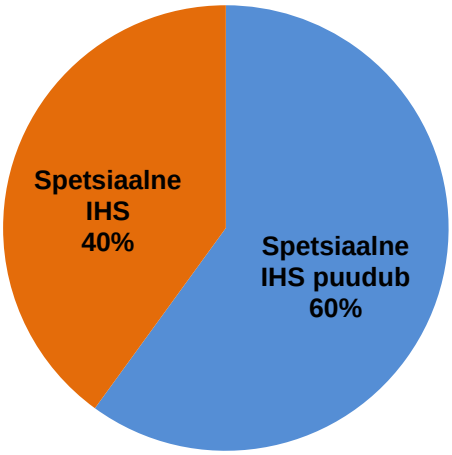
Joonis 20. Kasutajate andmete autentimiskeskkonda liikumise viiside jaotus.

Kasutajaandmete automaatne ülekandmine ei tähenda ilmtingimata spetsiaalse identiteedihaldussüsteemi olemasolu. Mitmetes asutustes on andmete liikumine lahendatud oma jõududega – on arendatud vastavad skriptid, mis loovad ühenduse personaliandmebaasiga, pärivad sealt andmed ja tõstavad need autentimiskeskkonda. Osades asutustes on rakendamisel või rakendatud lahendused, kus ettevõtte erinevad infosüsteemid jagavad omavahel kasutajate andmeid. Organisatsiooni tasemel ei leidunud ühtegi asutust, mis oleks rakendanud või rakendamas föderatiivset identiteedihalduse mudelit. On küll asutusi, kus on mitmed valitsemisala asutused koondatud ühtsesse süsteemi, kuid erinevaid identiteedi- ja pääsuõiguste halduse süsteeme, mis asuksid eraldiseisvates võrgukeskkondades ei leitud. Asutuste jaotust kolmandas peatükis kirjeldatud identiteedi mudelite järgi kujutab joonis 21.



Joonis 21. Identiteedi mudelite jaotus uuringus osalenud asutustes (föderatiivse ja globaalse identiteedi mudel uuringus osalenud asutustes puudub).

Spetsiaalne identiteedihaldussüsteem tuvastati uuringu käigus kahes asutuses – ühes on kasutusel kommertstarkvara, mille abil võetakse personalisüsteemist automaatselt kasutajaga seonduvad andmed, luuakse digitaalne identiteet, jagatakse see laiali liidestatud infosüsteemidesse ning hoitakse seda kogu identiteedi elutsükli jooksul värskena. Antud süsteem vastutab ka identiteetide kehtivuse eest ning vajadusel suleb kasutajakontod. Teises asutuses on kasutusel vabavaraline autentimiskeskkond ning identiteedi loomise ja elutsükli haldamisega tegelev infrastruktuur on ise arendatud. Spetsiaalse identiteedihaldussüsteemi olemasolu uuringus osalenud asutustes kirjeldab joonis 22.



Joonis 22. Spetsiaalsete identiteedihaldussüsteemide esinemine uuringus.

Eriala spetsialistidega suheldes, teoreetilise materjali läbitöötamise ja intervjuude käigus kerkisid esile mitmed head praktikad, mis väärivad märkimist:

- digitaalse identiteedi pärinemine personaliandmebaasist;
- kasutajate kehtivuse automaatne kontrollimine personaliandmebaasi abil;
- digitaalsete identiteetide atribuutide mitmekordse käsitsi sisestamise vältimine;
- hajussüsteemide arendamine, mis välistab ühese ründeobjekti tekke;
- avatud standardite ja protokollide kasutamine (näiteks Jasig CAS[67]), mis lihtsustavad arendamist ja liidestamist;
- IPH komponentide taaskasutamine, mis võib vähendada arendusmahtu- ja kulusid.

Osad väljatoodud parimatest praktikatest kehtivad ükskõik millises arendustegevuses ning pole uudsed, kuid nende seostamine identiteedi- ja pääsuõiguste haldusega on vajalik ja asjakohane.

Käesolevas peatükis anti ülevaade uuringu käigus kogutud andmetest, ettepanekutest analoogsetele uuringutele ja analoogsete uuringute metoodikale ning toodi välja töö käigus tuvastatud parimad praktikad identiteedi- ja pääsuõiguste halduses. Järgmises peatükis võetakse kogu töö autori poolt lühidalt kokku.

[67] www.jasig.org (CAS – Central Authentication Service)

KOKKUVÕTE

Töö tulemusena anti ülevaade identiteedi- ja pääsuõiguste haldusest, selgitati digitaalse identiteedi mõistet, selle elutsüklit, avati pääsuõiguste mõiste, tutvustati identiteedihalduse mudeleid ning võimalikke lahendusi ning viidi läbi uuring avalikus sektoris, et selgitada identiteedi- ja pääsuõiguste olukord asutustes ja infosüsteemides. Ühtlasi oli töö eesmärgiks tuvastada identiteedi- ja pääsuõiguste halduse parimaid praktikaid. Töö eesmärgiks ei olnud kirjeldada kõike identiteedi- ja pääsuõiguste haldusega seonduvat detailselt, vaid anda ülevaade teemast ning olulisematest mõistetest. Autori arvates on väga oluline mõista, mis on digitaalne identiteet ning selle roll pääsuõigustega seonduvates protsessides. Eriti oluline on see üleriiklikus võtmes, kus identiteedihalduse mõistlik korraldus võib tagada riigi avaliku ja erasektori koosvõime. Väga oluline on ka koosvõime ja koostöö teiste riikidega ning selle läbi saavutatav majanduslik suutlikkus, sest aina rohkem avalikke- ja erateenuseid liigub digitaalsesse maailma. Kindlasti pole riiklik identiteedi- ja pääsuõiguste halduse korraldamine lihtne ülesanne, kuid ID-kaardi, X-tee, STORK projektis osalemisega ning mitmete muude projektide käivitamisega ja avalike tugiteenuste loomisega on algus tehtud, nüüd on vaja ainult edasi liikuda. Millised võiksid olla riiklikud identiteedi- ja pääsuõiguste halduse lahendused? Identiteedi- ja pääsuõiguste haldust saab tehniliselt korraldada väga erinevalt. On võimalik luua üks keskne süsteem, mille nõrgaks küljeks on võimalus arendada ühtne ründeobjekt. On võimalik luua hajussüsteem, mille nõrgaks küljeks on aga võimalik süsteemi nõrga lüli olemasolu, mis võib vähendada süsteemi käideldavust. Samas on hajussüsteemide loomine tänapäeval väljakujunenud parimaks praktikaks ning seda propageeritakse ka riiklikul tasemel. Seega tehnilist lahendust välja pakkuda on keeruline ja see vajab kindlasti täiendavat analüüsi. Vaadeldes aga identiteedi- ja pääsuõiguste haldust korraldusliku poole pealt, tasub kindlasti riigis laiemalt analüüsida olukorda ning võimalik, et on teatud kohti, kus on vajalik ja võimalik universaalne ning ühetaoline üleriigiline lähenemine. Üheks väikeseks, kuid kindlasti oluliseks kohaks võiks olla näiteks riiklikult juurutatava finants- ja personalisüsteemi SAP liidese loomine, mida saaksid kõik SAPi kasutavad riigiasutused oma identiteedi- ja pääsuõiguste halduse süsteemides kasutada. Võimalik, et kaaluda tuleks keskse riigiametnike andmebaasi loomist, mille abil saaksid erinevad riiklikud infosüsteemid kontrolle teostada, et riiklikesse infosüsteemidesse ei pääseks volitamata kasutajad, näiteks kelle töösuhe on lõppenud, aga keda pole veel mingil põhjusel infosüsteemi kasutajate hulgast välja võetud. Selge on ka see, et kõikides riiklikes teenustes ei ole vajalik ega ka mõistlik kasutajate identiteedi tuvastamine, vaid vahel piisab ka pseudonüümist, kuna kõikide riiklike

teenuste puhul ei ole isikustamine vajalik. Võimalik, et mõningate teenuste puhul pole vajalik ka pseudonüüm, vaid piisab anonüümsest kasutajast. Seetõttu on riikliku identiteedi- ja pääsuõiguste halduse poliitika ja strateegia väljatöötamine keerukas ja mitmetahuline tehnilise, organisatoorse ja õigusliku iseloomuga küsimus.

Vaadeldes uuringus osalenud organisatsioone ning infosüsteeme üheskoos, võib öelda, et identiteedi- ja pääsuõiguste halduse parimad praktikad on rohkemal või vähemal määral kõikides uuringus osalenud asutustes ja infosüsteemides kasutusel. Identiteedi- ja pääsuõiguste realiseerimisel lähtutakse valdavalt hajussüsteemide põhimõttest, et välistada ühe ründeobjekti teket, kasutatakse avatud standardeid ja protokolle ning arenduskulude kokkuhoiuks taaskasutatakse olemasolevaid komponente, nagu ID-kaardi autentimismoodulid või lausa teise asutuse poolt loodud autentimisteenused (näiteks SAIS ja Eesti Teabevärav www.eesti.ee). Magistritöö uurimiseks püstitati 2 hüpoteesi:

Hüpotees 1: Avaliku sektori asutustes rakendatud identiteedi- ja pääsuõiguste halduse lahendused ei ole tänapäevased, nende arendamisel ei ole lähtutud parimatest praktikatest ning identiteedi- ja pääsuõiguste arendamisega avaliku sektori asutustes ei tegeleta piisavalt.

Hüpotees 2: Avaliku sektori asutuste identiteedi- ja pääsuõiguste haldamise taset on võimalik tõsta kui tuvastada ja juurutada parimad praktikad.

Organisatsioonide ja infosüsteemide taseme uurimisel selgus, et identiteedi- ja pääsuõiguste haldus on erinevates protsessilõikudes erinevalt korraldatud. Väga sarnaselt on lahendatud identiteedi loomine asutuse töötajatele – see saab alguse kõikidel juhtudel personaliandmebaasist. Personalibaasist alustamine on hea ja levinud praktika ning ühtlasi ka loomulik, sest värbamise käigus kogutakse andmeid, mis on identiteedi atribuutidena vajalikud. Loomulik on, et andmeid taaskasutatakse, mitte ei looda uuesti - ei nõuta korduvalt samade andmete sisestamist. Samas andmete ümbertõstmise meetod personaliandmebaasist on asutuste kaupa erinev, kuid ka siin on näha ühetaolisust – 60% puhul küsitletud asutustest käib see automaatselt. See avab ka seose asutuste suuruse ja IH korralduse vahel – automaatne identiteetide loomine on lahendatud suure kasutajate arvuga asutustes. Ka andmete järgmine samm on üsna ühesugune – neid hoitakse kataloogisüsteemis ning see on ka autentimise ja identifitseerimise ning autoriseerimise keskne puutepunkt. Uuringus kogutud andmed viitavad sellele, et IPH on üldiselt avaliku sektori asutustes korraldatud ühetaoliselt, IPH arendamisel lähtutakse üldjuhul parimatest praktikatest ning IPH temaatikale pööratakse märkimisväärset tähelepanu.

Infosüsteemide tasemel leiti mitmeid huvitavaid lahendusi. Näiteks Sisseastumise Infosüsteemi puhul lahendati autentimine ja identifitseerimine keskselt, kasutades eesti.ee portaali, Keskkonnateabe infosüsteemides on kasutusel keskne autentimismehhanism, samuti on mitmetes avaliku sektori organisatsioonides kasutusel keskne autentimismehhanism, mis on kujunenud heaks praktikaks. Samas selgus intervjuu käigus, et kõik infosüsteemid pole liidestatud kesksete autentimissüsteemidega. Loomulikult polegi kas andmeturbe või süsteemi eripärast tulenevalt vajalik ega mõistlik kõiki infosüsteeme ja andmekogusid alati siduda keskse autentimissüsteemiga. Küll aga suurendaks selline lähenemine kasutajamugavust ning tõstaks turvalisust. Mitmetes asutustes on kasutusel identiteediga seonduvate andmete õigena hoidmine erinevates süsteemides, kasutades kas metakataloogi või virtuaalkataloogi lahendust. Selline lahendus tagab andmete õigsuse ja usaldusväärsuse, vähendab käsitööd ning tõstab tootlikkust. Need kaks põhimõtet on head praktikad, mille juurutamisega oleks kindlasti võimalik tõsta tootlikkust ja efektiivsust. Antud uuringu raames polnud ressursside piiratuse tõttu võimalik tõestada nende praktikate juurutamise tulemusena saavutatavat võitu ning nende juurutamiseks kuluvate vahendite kulu-tulu suhet. On selge, et kui peab meeles pidama ühte kasutajanime ja parooli mitme asemel või sisestama enda kontaktandmeid ühe korra ühte süsteemi kui mitu korda erinevasse süsteemi, siis jääb rohkem aega töö tegemiseks. Kogutud andmed viitavad sellele, et parimad praktikad on olemas, neid rakendatakse ja nende laiema juurutamisega on võimalik suurendada töötajate produktiivsust, parandada identiteedi- ja pääsuõiguste haldamise taset ning infoturvet.

Üheks vahendiks ja instrumendiks parema IPH korraldamisel riigiasutustes on kindlasti Riigi Infosüsteemide Arenduskeskuse poolt arendatav ISKE etalonturbe raamistik, mida oleks otstarbekas IPH suunal täiendada. ISKE moodulites kajastatakse nii pääsuõiguste kontrollimist andmebaasides (ISKE moodul 5.7), kasutajaprofiilide seiret (moodulid 5.7, 5.8 ja 5.9), kuid mitmetel juhtudel nõutakse nende nõuete täitmist ainult H turbeastme puhul (meede HS.7). Enne ISKE täiendamist on kindlasti vaja välja töötada identiteedi- ja pääsuõiguste halduse riiklikud suunad ja põhimõtted ning viia läbi laiem ja sügavam identiteedi- ja pääsuõiguste halduse uuring Eesti avalikus sektoris.

KASUTATUD ALLIKAD

2AB. (2004). *What is Access Management?* Kasutamise kuupäev: 17.01.2011. a., allikas http://www.2ab.com/pdf/AccessManagement.pdf

Benantar, M. (2006). *Access Control Systems - Security, Identity Management and Trust Models.* Springer.

Bertino, E., & Takahashi, K. (2011). *Identity Management - Concepts, Technologies, and Systems.* Artech House.

Department of Defence. (1985). *http://csrc.nist.gov/.* Kasutamise kuupäev: 21.03.2011. a., allikas National Institute of Standards and Technology: http://csrc.nist.gov/publications/history/dod85.pdf

Elektroonilise teabeturbe ning eriside korraldamiseks ja kontrollimiseks kasutatavad meetodid ja vahendid. (29.01.2007. a.). Kasutamise kuupäev: 11.03.2011. a., allikas Riigi Teataja: https://www.riigiteataja.ee/akt/12783356

European eID Interoperability Platform . (2009). Kasutamise kuupäev: 31.01.2011. a., allikas https://www.eid-stork.eu/

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2007). *Role-Based Access Control (Second Edition).* Artech House, Inc.

Future of Identity in the Information Society (FIDIS). (2004). Kasutamise kuupäev: 17.01.2011. a., allikas http://www.fidis.net/

Goldsmith, I., & Mulqueen, T. (1999). *The Open Group.* Kasutamise kuupäev: 01.04.2011. a., allikas http://www.opengroup.org/comm/the_message/magazine/mmv5n2/meta.htm

Hanson, V., Laur, M., Buldas, A., & Nõgisto, I. (2011). *Andmekaitse ja infoturbe seletussõnastik Inglise-Eesti.* Cybernetica AS.

Jasig. (1999). *Jasig Central Authentication Service.* Kasutamise kuupäev: 31.01.2011. a., allikas http://www.jasig.org/cas

Maksu- ja Tolliamet. (2011). Kasutamise kuupäev: 05.03.2011. a., allikas Maksu- ja Tolliameti koduleht: http://www.emta.ee

McDuff, R., & McMillan, P. (06.05.2006. a.). *An Identity and Access Management Framework for Australian and New Zealand Higher Education and Research.*

Kasutamise kuupäev: 08.02.2011. a., allikas http://www.caudit.edu.au/educauseaustralasia09/assets/presentations/wednesday/Patricia%20McMillian%20&%20Rodney%20McDuff.pdf

McKenzie, R., Crompton, M., & Wallis, C. (2008. a.). *Use Cases for Identity Management in E-Government.* Kasutamise kuupäev: 09.03.2011. a., allikas http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2008.51

OASIS. (2011). *OASIS: Advanced open standars for the global information society*. Kasutamise kuupäev: 15.04.2011. a., allikas http://www.oasis-open.org/

Parmakson, P. (2011). Identiteedi- ja pääsuhalduse uurimine: metoodika.

Portaal arenguhuvilisele juhile. (2011). Kasutamise kuupäev: 02.04.2011. a., allikas Infoturve: http://www.juhtimine.ee/infoturve

Põhja-Eesti Regionaalhaigla. (2011). Kasutamise kuupäev: 31.03.2011. a., allikas http://www.regionaalhaigla.ee

Reed, A. (2002). *The Definitive Guide to Identity Management.* realtimepublishers.com.

Registrite ja Infosüsteemide Keskus. (2011). Kasutamise kuupäev: 31.03.2011. a., allikas http://www.rik.ee

RIA. (13.01.2011. a.). *X-tee 5.0 turvaserveri kasutusjuhend.* Kasutamise kuupäev: 03.04.2011. a., allikas ftp://ftp.aso.ee/pub/x-tee/v5/docs/est/turvaserveri_kasutusjuhend.pdf

Riigi Infosüsteemi Arenduskeskuse põhimäärus. (26.09.2009. a.). Kasutamise kuupäev: 25.02.2011. a., allikas Riigi Teataja: https://www.riigiteataja.ee/akt/13219897

Siseministeeriumi Infotehnoloogia- ja Arenduskeskus. (2011). Kasutamise kuupäev: 10.04.2011. a., allikas http://www.smit.ee

Structured Overview on Prototypes and Concepts of Identity Management Systems. (2005). Kasutamise kuupäev: 14.03.2011. a., allikas www.fidis.net: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf

The Global Information Technology Report 2009–2010. (2010). Kasutamise kuupäev: 25.02.2011. a., allikas http://www.networkedreadiness.com/gitr/main/fullreport/index.html

Todorov, D. (2007). *Mechanics of User Identification and Authentication: Fundamentals of Identity Management.* Auerbach Publications.

TRB Access Management Commitee Home Page. (2011). Kasutamise kuupäev: 10.03.2011. a., allikas http://www.accessmanagement.info/

Wikipedia.org, Access control. (22.01.2011. a.). Kasutamise kuupäev: 31.01.2011. a., allikas http://en.wikipedia.org/wiki/Access_control

Wikipedia.org, Business to business (B2B). (11.01.2011. a.). Kasutamise kuupäev: 31.01.2011. a., allikas http://en.wikipedia.org/wiki/Business-to-business

Wikipedia.org, Business to government. (30.09.2010. a.). Kasutamise kuupäev: 31.01.2011. a., allikas http://en.wikipedia.org/wiki/Business-to-government

Wikipedia.org, Federated identity. (16.01.2011. a.). Kasutamise kuupäev: 31.01.2011. a., allikas http://en.wikipedia.org/wiki/Federated_identity

Wikipedia.org, Identity management. (10.01.2011. a.). Kasutamise kuupäev: 02.02.2011. a., allikas http://en.wikipedia.org/wiki/Identity_management

Wikipedia.org, Role based access control. (23.01.2011. a.). Kasutamise kuupäev: 25.01.2011. a., allikas http://en.wikipedia.org/wiki/Role-based_access_control

Wikipedia.org, Security Assertion Markup Language (SAML). (24.01.2011. a.). Kasutamise kuupäev: 31.01.2011. a., allikas http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

Wikipedia.org, Two-factor authentication. (10.04.2011. a.). Kasutamise kuupäev: 13.04.2011. a., allikas Wikipedia: http://en.wikipedia.org/wiki/Two-factor_authentication

Williamson, G., Yip, D., Sharoni, I., & Spaulding, K. (2009). *Identity Management A Primer.* MC Press Online.

Windley, P. (2005). *Digital Identity.* O'Reilly.

SUMMARY

Master thesis

IDENTITY AND ACCESS MANAGEMENT IN ESTONIAN PUBLIC SECTOR

Estonia started to develop its systems and infrastructure in prime time, at the time, when many technologies became mature and widely available. It is also one of the reasons why IT development in Estonia has been so rapid. Its rapid development has been at the heart of the country's authorities, who administer the national databases containing personal information, state secrets, tax secrets, and other information to which access must be limited and users identified. Identity and access management issues become more and more important in Estonian public sector as there are more regulations on the subject and more training on data protection awareness. On the other hand, structural funds and subsidies, requirements on systems and software development accompanied by affiliation with European Union, have intensified software and systems development process. As a result, number of information systems and web services is increasing rapidly, among which there are many public information systems and services. This in turn, creates a situation where information systems users, in addition to their individual identities (Skype, MSN, Gmail, Facebook etc.) have lots of identities in public information systems and databases, which means, that the focus in the future will be on identity management issues.

Main goal of this master thesis is to clarify identity and access management-related concepts, methods and policies, and with the help of selected case studies examine identity and access management situation in the Estonian public sector. Goal is to obtain useful and usable overview of identity and access management methods and technical solutions in Estonian public sector, using a limited selection of Estonian public institutions and information systems. Additional objective is to identify best practices of identity and access management, distribute and introduce them using current master thesis.

Identity and access management is strongly linked to other IT areas, such as user rights management, information security, software development and others. Since identity and access management is complex and substantial information technology issue, it is clear, that research objectives need to be tightened, because everything topic-related is not feasible to research. Selection of public institutions and public information systems may seem minor and topic itself simple, but actually the topic is broad and complex. Estonian terminology regarding identity and access management is poorly developed, solutions and processes are

complex and topic is previously unexplored. Thorough review of theoretical material and carefully selected selection of public institutions and public information systems should be sufficient to provide necessary overview of identity and access management in Estonian public sector. Knowledge which is planned to collect with this master thesis is summarized as two hypotheses:

Hypothesis 1: Identity and access management solutions implemented in Estonian public sector are not modern, development of identity and access management solutions do not base on best practices and public sector institutions do not address identity and access management issues adequately.

Hypothesis 2: It is possible to amend level of identity and access management in Estonian public sector, if best practices are identified and implemented.

Data collected from study refers, that identity and access management in Estonian public sector is organized similarly, identity and access management development is based on best practices and identity and access management issues are addressed adequately.

Collected data indicates that best practices exist, they are implemented and their wider introduction can increase employee productivity and improve level of identity and access management and information security.

LÜHENDID

IT - infotehnoloogia

ISKE – Infosüsteemide kolmeastmeline etalonturbe süsteem

IPH – identiteedi – ja pääsuõiguste haldus, ingl k IAM – identity and access management

IH – identiteedihaldus, ingl k identity management

PÕH – pääsuõiguste haldus, ingl k access management

IHS – identiteedihalduse süsteemid

MÕISTED

Atribuut – oluline, lahutamatu tunnus; juurdekuuluv ese, tarvik (ÕS 2006)

Subjekt – isik (ÕS 2006)

Olem – infosüsteemiga kirjeldatava süsteemi v valdkonna konkreetne v abstraktne komponent, kontseptuaalmudeli põhielement (ÕS 2006)

Infoturve - infoturve on teabe ja infosüsteemide kaitsmine loata juurdepääsu, kasutamise, avaldamise, muutmise või hävitamise eest (Portaal arenguhuvilisele juhile, 2011)

Privaatsus – isiku või rühma võime soovitud ulatuses isoleerida teistest ennast või teavet enda kohta, avalikustades end valikuliselt; privaatseks loetava piirid ja sisu erinevad kultuuriti ja isikuti. (Hanson, Laur, Buldas, & Nõgisto, 2011)

JOONISED JA TABELID

Lisa 1 Organisatsiooni küsimustik

Sissejuhatavad küsimused

- Kui palju on kasutajaid?
- Kas on ka väliskasutajaid?
- Kui palju on infosüsteeme?
- Kas infosüsteemid kasutavad teiste infosüsteemide andmeid?
- Kes on infosüsteemide kasutajad?
- Kas infosüsteemide puhul on kasutusel kasutajagrupid?
- Kas infosüsteemide puhul kasutatakse rolle?
- Kas infosüsteemide puhul on ka väliskasutajaid?

Tehnoloogiline aspekt

- Mismoodi on andmekogudele ligipääs üles ehitatud?
- Kas kõik infosüsteemid kasutavad ühte autentimiskeskkonda või on kasutusel mitmed autentimiskeskkonnad?
- Kust saavad kasutajate andmed alguse?
- Mismoodi jõuavad kasutajate andmed autentimiskeskkonda?
- Kas on tegemist käsitööga või on andmete liigutamine automatiseeritud?
- Kui on kasutusel mitu autentimiskeskkonda, siis kas nende keskkondade vahel liigub kasutajaid puudutav informatsioon?
- Kas identiteetide haldamiseks kasutatakse spetsiaalseid tehnilisi lahendusi?
- Millise lahenduse või tootega tegemist on?
- Kas IPH realiseerimisel kasutati tänapäevaseid ja uuenduslikke lahendusi ning arhitektuure?

Infoturbe ja andmekaitse aspekt

- Milliseid vahendeid kasutatakse kasutajate identifitseerimiseks?
- Kas infoturbetasemed on identifitseeritud ja IPH lahendus on selle järgi üles ehitatud?
- Kas IPH lahendused tagavad nõutava infoturbetaseme?
- Kas andmekaitse nõuete täimine on tagatud?

Sotsiaalne aspekt

- Kes on IPH lahenduste kasutajad?

- Kas IPH lahendused on sotsiaalselt aktsepteeritud ja järgitud, kas ja kuidas on kooskõlas organisatsiooni kultuuriga, Eesti kultuuri ja tavadega laiemalt, sh ootustega privaatsusele, avalikkusele ja läbinähtavusele?
- Kas IPH lahenduse loomisel on arvestatud sotsiaalse aspektiga?

Funktsionaalne aspekt

- Millised talituslikud eesmärgid olid hankimisel IPH lahendusele seatud?
- Mida teeb IPH lahendus praegu?
- Kas IPH lahendus täidab seatud eesmärke?

Kasutatavuse aspekt

- Kas IPH lahendused on mugavad kasutada?
- Kas IPH kasutajad on lahendusega rahul?
- Kas ja kuidas IPH lahendusi tegelikult kasutatakse?
- Kas IPH lahenduse kasutatavuse või kasutusmugavuse osas on parendusettepanekuid?

Õigusliku regulatsiooni aspekt

- Millised õigusaktid reguleerivad kasutusel oleva IPH lahenduse tööd?
- Kas IPH lahenduse tööd reguleerib mõni asutuse sisemine kord või eeskiri?
- Kas IPH lahenduses töödeldakse tundlikke andmeid, näiteks isikuandmeid, riigisaladust?

Majanduslik aspekt

- Kas IPH lahendused on kuluefektiivsed?
- Kas IPH lahenduse hankimisel tehti tasuvusanalüüs?
- Kas IPH lahenduse juurutuse järgselt tehti järelhinnang, kus võrreldi kas algne tasuvusanalüüs vastas tõele?
- Kas IPH on korraldatud ilma ebavajaliku dubleerimiseta?
- Kas oskusteave kantakse üle ja on taaskasutatav?

Lisa 2 Infosüsteemi küsimustik

Sissejuhatavad küsimused

- Kes on infosüsteemi kasutajad?
- Kas infosüsteemi puhul on väliskasutajaid?
- Kas infosüsteemi puhul on kasutusel kasutajagrupid?
- Kas infosüsteemis on kasutatusel rollid?

Tehnoloogiline aspekt

- Mismoodi on infosüsteemile ligipääs üles ehitatud?
- Kas infosüsteem kasutab ühte autentimiskeskkonda või on kasutusel mitmed autentimiskeskkonnad?
- Kust saavad alguse kasutajate andmed?
- Mismoodi jõuavad kasutajate andmed autentimiskeskkonda?
- Kui on kasutusel mitu autentimiskeskkonda, siis kas nende keskkondade vahel liigub kasutajaid puudutav informatsioon?
- Kas identiteetide haldamiseks kasutatakse spetsiaalset tehnilist lahendust?
- Millise lahenduse või tootega tegemist on?
- Kas IPH realiseerimisel kasutati tänapäevaseid ja uuenduslikke lahendusi ning arhitektuure?

Infoturbe ja andmekaitse aspekt

- Milliseid vahendeid kasutatakse kasutajate identifitseerimiseks?
- Kas on kasutusel mitmeid meetodeid kasutajate identifitseerimiseks?
- Kas infoturbetasemed on identifitseeritud ja IPH lahendus on selle järgi üles ehitatud?
- Kas IPH lahendused tagavad nõutava infoturbetaseme?
- Kas tagatakse andmekaitse nõuete täimine?

Sotsiaalne aspekt

- Kes jagab ligipääse?

- Kas IPH lahendused on sotsiaalselt aktsepteeritud ja järgitud, kas ja kuidas on kooskõlas organisatsiooni kultuuriga, Eesti kultuuri ja tavadega laiemalt, sh ootustega privaatsusele, avalikkusele ja läbinähtavusele?
- Kas IPH lahenduse loomisel on arvestatud sotsiaalse aspektiga?

Funktsionaalne aspekt

- Millised talituslikud eesmärgid olid hankimisel IPH lahendusele seatud?
- Kas IPH lahendus teeb seda, mida hankimisel lahenduselt oodati?
- Kas IPH lahendus täidab seatud eesmärke?

Kasutatavuse aspekt

- Kas IPH lahendus on mugav kasutada?
- Kas IPH kasutajad on lahendusega rahul?
- Kas ja kuidas IPH lahendusi tegelikult kasutatakse?
- Kas IPH lahenduse kasutatavuse või kasutusmugavuse osas oleks parendusettepanekuid?

Õigusliku regulatsiooni aspekt

- Millised õigusaktid reguleerivad kasutusel oleva IPH lahenduse tööd?
- Kas IPH lahenduse tööd reguleerib mõni asutuse sisemine kord või eeskiri?
- Kas IPH lahenduses töödeldakse tundlikke andmeid, näiteks isikuandmeid, riigisaladust?
- Kas ja kuidas on IPH lahenduse puhul tagatud seaduslikkus?

Majanduslik aspekt

- Kas IPH lahendus on kuluefektiivne?
- Kas IPH lahenduse hankimisel tehti tasuvusanalüüs?
- Kas IPH lahenduse juurutusjärgselt tehti järelhinnang, kus võrreldi kas algne tasuvusanalüüs vastas tõele?
- Kas IPH on korraldatud ilma ebavajaliku dubleerimiseta?
- Kas oskusteave kantakse üle ja on taaskasutatav?

Lisa 3 Intervjuude töötlemise tabel

Sissejuhatavad	
Infosüsteemide arv	number
Sidustus teiste infosüsteemidega	jah/ei
Sisemiste infosüsteemide kasutajate arv	number
Infosüsteemide kasutajad	sisemised/välimised
Kas kasutatakse rolle?	jah
Tehnoloogiline	
Mismoodi on ligipääs üles ehitatud?	näiteks rollipõhine, kasutajad valdavalt infosüsteemi juures
Autentimiskeskkonnad	üks/mitu
Kasutajaandmete algus	näiteks personaliandmebaas
Kasutajaandmete liikumine autentimiskeskkonda	käsitsi/automaatselt/nii käsitsi kui ka automaatselt
Info liikumine autentimiskeskkondade vahel	ei liigu/liigub automaatselt/liigub käsitsi/osaliselt automaatselt/osaliselt käsitsi
IPH spetsiaalne tehniline lahendus	jah/ei
Spetsiaalse IPH toote nimetus	näiteks Microsoft Forefront Identity Manager
Infoturve ja andmekaitse	
Identifitseerimise viisid	kasutajanimi/parool/kiipkaart/ID kaart
Infoturbetasemed olemas ja identifitseeritud	näiteks ISKE ja sisemine kord
Kas IPH tagab nõutava turvataseme	jah/ei
IPH lahenduse andmekaitse nõuete täimine on tagatud?	jah/ei
Sotsiaalne	
Kes jagab õigusi?	peakasutajad/IT
Ootused privaatsusele?	näiteks ootused privaatsusele on uuritud, need on täidetud/pole uuritud
Sotsiaalne aspekt?	ei oska hinnata
Funktsionaalne	
Talituslikud eesmärgid hankimisel?	dokumenteeritud/pole dokumenteeritud
Kas täidab eesmärke täna?	järelhinnang on läbi viidud/järelhinnangut pole läbi viidud
Kasutatavus	
Kas IPH lahendused on mugavad kasutada?	on uuritud/ei ole uuritud
Kas kasutajad on rahul?	on uuritud/ei ole uuritud
Kas ja kuidas tegelikult kasutatakse?	on uuritud/ei ole uuritud
Kas on kasutusmugavuse osas ettepanekuid?	jah/ei
Õiguslik regulatsioon	
Millised õigusaktid reguleerivad?	iske ja sisemine kord
Tundlikke andmeid töödeldakse?	jah/ei
Seaduse täitmine on tagatud?	jah/ei
Majanduslik	
Kas IPH lahendused on kuluefektiivsed?	jah/ei/pole hinnatud
Kas hankimisel tehti tasuvusanalüüs?	jah/ei
Kas on tehtud järelhinnang?	jah/ei
On korraldatud ilma ebavajaliku dubleerimiseta?	jah/ei
Oskusteave kantakse üle ja on taaskasutatav?	jah/ei