PROUD ENGINEERS

Keskne volituste, rollide ja pääsuõiguste haldamise süsteem

Hetkeolukorra kaardistus ja analüüs

Koostaja: Proud Engineers OÜ

Versioon: 1.0

Kuupäev: 14.12.2021

Proud Engineers OÜ | Kristjani tee 4, 74015 Miiduranna, Estonia
getstarted@proudengineers.ee | proudengineers.ee

Sisukord

Kasutatud mõisted ja lühendid

ABAC	Ing. k *Attribute-Based Access Control* ehk atrbibuudipõhine pääsuhaldus , vt. atribuudipõhine pääsuhaldus
ACL	Ing. k *Access Control List* ehk pääsuloend, vt. pääsuloendi põhine pääsuhaldus
Atribuudipõhine pääsuhaldus	Pääsuhalduse mudel, mille puhul määrab kasutaja õiguse konkreetse toimingu sooritamiseks mõni kasutaja omadus, näiteks vanus.
FIE	Füüsilisest isikust ettevõtja äriseadustiku § 3 tähenduses
MISP2	X-tee valmiskomponent, mis võimaldab kasutajal automaatselt luua ja kasutusele võtta kasutajaliidesed x-tee teenuste kasutamiseks
MTA	Maksu ja- Tolliamet
PPA	Politsei- ja Piirivalveamet
Pääsuloendi põhine pääsuhaldus	Pääsuhalduse mudel, mille puhul määrab kasutaja õiguse konkreetse toimingu sooritamiseks tema kuulumine vastava õigusega kasutajate nimekirja
RBAC	Ing. k *Role-based Access Control,* ehk rollipõhine pääsuhaldus vt. rollipõhine pääsuhaldus
RIK	Registrite ja Infosüsteemide Keskus
Rollipõhine pääsuhaldus	Pääsuhalduse mudel, mille puhul määrab kasutaja õiguse konkreetse toimingu sooritamiseks tema määratus mingisse konkreetsesse rolli
RTK	Riigi Tugiteenuste Keskus

SaaS	Ing. k *Software-as-a-Service*, ehk viis, kus klient saab kaugpääsuga kasutada teenuseandja rakendusi.
SAP	RTK poolt hallatav majandustarkvara
SLA	Ing. k *Service Level Agreement* ehk teenustaseme lepe
TARA	Riigi autentimisteenus
TEHIK	Tervise ja Heaolu Infosüsteemide Keskus

1. Sissejuhatus

Majandus- ja Kommunikatsiooniministeeriumi tellimusel valmis aastal 2020 ettevõtja ühtse veebipõhise kontaktpunkti tulevikuvaade koos arendus- ja tegevusplaaniga (teekaart), ettevõtjate sündmusteenuste arendamise analüüsi ning kontaktpunkti prototüübiga.[1] Peamiste murekohtadena toodi välja, et:

- Avaliku sektori osutatavate teenuste, toetuste ning seatud kohustuste info on killustatud ja sageli raskesti leitav, mõnikord ka vananenud; ja
- Palju aega kulub tuvastamaks, kelle poole pöörduda probleemi kiireimaks lahendamiseks; ja
- Asutustele andmete esitamise koormus on kõrge; ja
- Puudub ühtne ja terviklik ülevaade riigis pakutavatest avalikest teenustest.

Lahendusena pakuti välja ühtse ettevõtja kontaktpunkti kontseptsioon, kus ettevõtjale suunatud e-teenused, info ja asjaajamine jm saaks toimuda tervikteenusena „ühest aknast" eesti.ee portaalist nii riigi sees kui ka piiriüleselt.[2] Ühtse kontaktpunkti kaudu soovitakse vähendada ettevõtja halduskoormust ja bürokraatiat.

Kontaktpunkti funktsionaalsusena on muuhulgas välja toodud ka lahendus, mille abil saab ettevõtja hallata volitusi, rolle ja pääsuõigusi ühes kohas keskselt.[3] Aprillis 2021.a avaldas RIA avatud hankemenetluse „Pääsuhalduste analüüs" (viitenumber 235557) eesmärgiga analüüsida olemasolevaid pääsuhalduse lahendusi, vajadusel välja pakkuda uus keskne pääsuhalduslahendus ning analüüsida vajalikke muudatusi õigusruumis. Edukaks pakkujaks tunnistati Proud Engineers OÜ.

Pakkumuse kohaselt toimuvad tööd projekti käigus kahes etapis, millest esimeses viiakse läbi olemasolevate volituste, rollide ja pääsuõiguste lahenduste analüüs. Käesolev dokument on nimetatud esimese etapi töid ja tulemeid kirjeldav kokkuvõte.

Analüüsi eesmärk oli leida vastused järgmistele pakkumuse punktis 2.1 nimetatud uurimisküsimustele:

1. Mis on ettevõtjate peamised vajadused ja probleemid? (vt p 3); ja

[1] „Ettevõtjate jaoks ühtse veebipõhise kontaktpunkti visioon" ja selle lisad, https://pilv.mkm.ee/s/ZRQQB89TRJZjiYn (25.08.21).
[2] „Ettevõtjate jaoks ühtse veebipõhise kontaktpunkti visioon", lk 11-12.
[3] „Ettevõtjate jaoks ühtse veebipõhise kontaktpunkti visioon", lk 12.

2. Missuguseid olemasolevaid pääsuhalduslahendusi kasutatakse (mille jaoks lahendust kasutatakse, millised on rollid, millistel põhimõttel rolle jagatakse ja õigusi rollidele määratakse, milline on tehniline lahendus? (vt p-d 4.1-4.2);
3. Milline on sobivaim lahendus edasiliikumiseks (vt p 4.3.4); ja
4. Missugused teenuskeskkonnad kasutavad pääsuhalduslahendusi? (vt p 5).

2. Metoodika

Sissejuhatuses kirjeldatud uurimisküsimustele vastamiseks analüüsiti nii avaliku sektori teenusepakkujate olemasolevaid lahendusi kui ka ettevõtjate vajadusi ja probleeme pool-struktureeritud intervjuude käigus.

Olemasolevate pääsuhalduslahenduste kaardistamiseks mõeldud intervjuu küsimustiku leiab lisast 1 (vt. Lisa 1 - Intervjuu küsimused). Lisaks küsimustikule, mis on aluseks olemasolevate lahenduste võrdlusele (vt p-d 4.1-4.2), dokumenteeriti üldisi märkusi keskse pääsuhalduse kohta ning paluti intervjueeritavatel selgitada pääsuhaldust ümbritsevaid äriprotsesse organisatsioonis või haldusalas.

Sõltuvalt intervjueeritava organisatsiooni suurusest võis käsitletav süsteem ulatuda konkreetset infosüsteemist (näiteks riigihangete register) kuni terve haldusalani (näiteks TEHIK). Funktsionaalsuse mõttes oli skoop piiritletud lõppkasutaja pääsuõiguste haldusega; samas oli teenusepakkujaid, kes kaasasid ka sisemiste kasutajate pääsuõigustega tegelevaid ametnikke.

Ettevõtjate vajaduste kaardistamiseks viidi läbi intervjuud ettevõtetega, keda võib mõtteliselt jagada kolme persoona-gruppi (üks intervjueeritav ettevõte võis kuuluda ka mitmesse gruppi):

- Persoona 1: Ettevõtted, kes pakuvad olemasolevas pääsuhalduse kontekstis arendus- ja SaaS-teenuseid (kolm ettevõtet); ja
- Persoona 2: Ettevõtted, kes kasutavad pääsuhalduse lahendusi oma teenuse pakkumiseks, näiteks raamatupidamisteenused ja õigusalased konsultatsioonid (kaks ettevõtet; intervjuusid täiendati Eesti Raamatupidajate Kogu juhatuse liikmelt saadud infoga.); ja

- Persoona 3: Ettevõtted, kes kasutavad pääsuhalduse lahendusi oma ettevõtte haldamiseks ja juhtimiseks (neli ettevõtet).

Intervjueeritud ettevõtted on loetletud lisas 3 (Lisa 3 - Läbi viidud intervjuud).

3. Ettevõtete vajaduste ja probleemide kirjeldus

Ettevõtjatega tehtud intervjuudele seati järgnevad eesmärgid:

1. Valideerida ettevõtja ühtse kontaktipunkti analüüsi[4] järeldusi (kas tuleb välja midagi, mis läheks eelanalüüsis leituga vastuollu?); ja
2. Täpsustada ettevõtjate ootuseid pääsuhalduse funktsioonide osas; ja
3. Valideerida lahenduste kaardistuse käigus kogutud infot (vt p 4 all) arenduspartneritega; ja
4. Täpsustada arenduspartnerite ootuseid uue lahenduse osas.

3.1 Intervjuude leiud

Juhime tähelepanu, et allpooltoodud intervjuude leiud on nummerdatud viitamise mugavuse eesmärgil. Nummerdus ja leidude järjekord ei indikeeri leidude olulisust. Kaudselt võib olulisuse indikaatorina kasutada sõnastatud leiu mainimise sagedust (mitu intervjueeritavatest seda mainis), kuid kõike leide tuleks käsitleda kvalitatiivse tervikkogumina.

Persoona 1:

1. Ettevõttel on vajadus kasutada uut pääsuhalduslahendust ka x-tee kontekstis. SaaS teenuse puhul annaks selline esindusõiguse kontroll parema turvalisuse ning suurema paindlikkuse võimaldades lõppkliendil sujuvalt oma suhet teenusepakkujaga juhtida (2 ettevõtet 3-st).
2. Arenduspartneril on vajadus lahendada olukord, kus isiku roll ja õigused sõltuvad tema mõnest teisest seosest (inimene eraisikuna ei oma teatud teenusele ligipääsu kuid KOVi esindajana pääseb ta teenusele ligi). (1 ettevõte 3-st).

[4] „Ettevõtjate jaoks ühtse veebipõhise kontaktpunkti visioon" ja selle lisa 2.3.7, https://pilv.mkm.ee/s/ZRQQB89TRJZjiYn.

Persoona 2:

3. Senist detsentraliseeritud pääsuhalduse lahendust peetakse rahuldavaks või pigem ebamugavaks. Erandina tuuakse välja MTA, kelle lahendust peetakse rahuldavaks või pigem heaks (2 ettevõtet 2-st).
4. Puuduvad ootused pääsuhalduse lahenduse parendamiseks. Vajaduste loetelu on lühike ja tüüpiline ja nad on leidnud oma vajaduste elluviimiseks piisavalt head töövõtted (nt register kehtivate ligipääsude info haldamiseks või kasutusjuhend klientidele) (2 ettevõtet 2-st).
5. Pääsuhalduse väärkasutamisega seotud riske peetakse oluliseks. Riskide maandamiseks võetakse hoiak, et teenusepakkujale on antud minimaalselt vajalik arv volitusi (2 ettevõtet 2-st).
    a. Näiteks raamatupidajad eelistavad lahendust, kus raamatupidaja ei saa kas üldse ettevõtte pangakontole ligi või vähemalt ei saa maksekorraldusi ainuisikuliselt kinnitada.
    b. Advokaadibüroo esindaja sõnul on esindusõigus oluline õiguslik küsimus, mida kliendisuhte alguses soovitakse paika panna. Samas on menetlusosalise esindamine reguleeritud menetlusseadustikega (nt haldusmenetluse seadus, tsiviilkohtumenetluse seadustik) ning enamikel juhtudel advokaadist esindaja esindusõigust eeldatakse. Advokaadibüroo esindaja sõnul on esindusõiguse riskid olulised ning seistakse hea selle eest, et esindusõigus oleks alati olemas ning selle ulatust ei ületataks (vajadusel räägitakse segadust tekitavad küsimused enne kliendiga läbi).

Persoona 3:

6. Vajadus saada pääsuhaldusega seotud infot ning hallata pääsuhaldusega seotud funktsioone on ettevõtjate jaoks madala prioriteediga vajadus. Seda ei nimetata omaalgatuslikult kui olulist funktsooni, mis vajaks parandamist (3 ettevõtjat 4-st).

7. Ettepanek koondada pääsuhaldusega seotud info ja funktsioonid ühtsesse kesksesse lahendusse on ettevõtjate jaoks teretulnud ettepanek, kuid seda ei peeta hädavajalikuks (4 ettevõtjat 4-st).
8. Ootused pääsuhalduse mugavale ja ülevaatlikule lahendusele on kõige suuremad seoses pangateenuse kasutamise ja maksude deklareerimisega. Kõige olulisemad teenusepakkujad on Äriregister, MTA ja kommertspangad (3 ettevõtet 4-st).
9. Olulistest teenusepakkujatest kaks – MTA ja kommertspangad – on enda teenusega seotud pääsuhalduse juba praegu lahendatud heal tasemel (3 ettevõtet 4-st).
10. Kui pääsuhalduse funktsioone on mingil põhjusel vaja (ettevõttega seotud sündmus, teenusepakkuja vahetamine), võetakse seda kui praktilist natuke peavalu pakkuvat ülesannet (3 ettevõtet 4-st).
11. Ettevõtjad ei teadvusta pääshalduse väärkasutamisega seotud riske. Potentsiaalsele riskile ei ole intervjuule eelnevalt teadlikult mõelnud (3 ettevõtet 4-st).
12. Pääsuhalduse väärkasutamisega seotud riske ei peeta kriitiliseks. Suur osa intervjueeritavatest vastas, et nad ei tea täpselt, kes saab nende ettevõtte nimel mis keskkondadesse siseneda või milliseid toiminguid teha. Samas vastasid nad, et see olukord ei häiri neid (3 ettevõtet 4-st).
13. Pääsuhalduse väärkasutamisega seotud riske tunnetatakse kõige enam pangateenuse puhul. Selle teenuse ligipääsu piiratakse juba eos kõige rohkem ja selle teenuse puhul teatakse ligipääsuõiguse staatust üldjuhul peast (3 ettevõtet 4-st).
14. Punktis 13 tooduga samaväärsena ei tooda välja teisi oluliseks peetud teenuseid – äriregister ja MTA. Nende puhul ei peeta väärkasutamise riski nii oluliseks ja ootused ligipääsude asjakohasusele on madalamad (nt intervjueeritav tõi välja, et see ei pane teda muretsema kui mõni varasem raamatupidamisteenuse pakkuja saab MTA teenusele ligi ka pärast koostöö lõppemist) (2 ettevõtet 4-st).

3.2 Intervjuude järeldused ja soovitused

Investeeringu tasuvus

Ettevõtjatel on kõrged ootused avaliku ja erasektori e-teenuste kasutajamugavuse ja väärtuspakkumise osas. Ootuste teravik on aga suunatud teadlikkusele teenuste sisu osas ja teenuste enda kasutajamugavusele. Kõik Persoona 3 grupis ettevõtjad tõid kriitilise probleemina välja, et eelkõige on neil keeruline leida, millises teenuses/rakenduses milliseid toiminguid teostada ning erinevate toimingute teostamise lihtsus ja mugavus.

See järeldus toetab ühtse ettevõtja kontaktpunkti kontseptsiooni peamisi järeldusi (vt p 1), mille kohaselt on suuremaks probleemiks info ja teenuste üldine kättesaadavus ning tervikvaate puudumine, kui pääsuhalduse küsimused.

Pääsuhaldusega seotud küsimused on selgelt teise järgu probleem ja ootused juurutatava lahenduse osas on madalad. Seetõttu on oluline jälgida, et pääsuhalduse kesksesse lahendusse investeeritavad ressursid (rahaline, kommunikatiivne) oleks tasakaalus potentsiaalselt saavutatava efektiga.

Ettevõtjad ootavad, et riik investeerib lahendustesse, mis aitavad tal lihtsalt ja kiirelt:

A. aru saada, kus keskkonnas saab teostada toimingut X; ning
B. teostada toimingut X.

Oluliselt vähemtähtsam on:

C. saada infot selle kohta, kes saab teostada toimingut X.

C lahendamine toob kindlasti teatud positiivse efekti, kuid kui A ja B jäävad samal ajal tähelepanuta, on efekt väike. Kui C lahendamiseks kulutatakse aga (ettevõtja arvates) liialt ressursse, nullib see kogu positiivse efekti.

Mugavusfunktsioonid

Kuna pääsuhalduse temaatika on ettevõtja jaoks madala prioriteediga, on ka võimalikud uue lahenduse funktsioonid ja eelised tihti teadvustamata. Ettevõtjatel puudub nn soovinimekiri, mida uus lahendus võiks teha. Intervjuude käigus kirjeldati analüüsi autorite poolt ka ise võimalikke uue lahenduse mugavusfunktsioone – näiteks võimalust ühe liigutusega teatud isikult kõik ligipääsud eemaldada (lepingulise suhte lõpetamise tõttu) või kanda ühe isiku ligipääsud teisele (töötaja vahetamine). Sellisel juhul said lahendused tüüpiliselt positiivse hinnangu. Lisaks on ettevõtjatel, kes pääsuhaldust oma töös rohkem vajavad (Persoona 2), kasutusele võetud mõningad lahendused, millega ollakse küll rahul,

kuid mis võiks tulevikus olla lahendatud keskse usaldusväärse lahendusega (näiteks ülevaade kehtivatest rollidest ja teenustele ligipääsust).

Soovitame kaasata erinevad mugavusfunktsioonid rakenduse esmalahenduse skoopi, et tulevaste lahenduse sisulised eelised jõuaks lõppkasutajateni isegi siis, kui nad seda spetsiifilise ootusena ise defineerida ei oska.

Keskse lahenduse kättesaadavus

Kui tutvustada keskse pääsuhalduse erinevaid (potentsiaalseid) väärtuspakkumisi, peetakse info ühest kohast kättesaamist väärtuslikuks. Samas ei erista ettevõtja, kas teenuse omanik on riigiasutus või erasektori ettevõte. Nii näiteks on pangad üks esimesi teenusepakkujaid, keda pääsuhalduse vajaduse kontekstis mainitakse. Ettevõtjale sisulise väärtuse loomiseks tuleks võimaldada ja ärgitada, et kesksesse lahendusse oleks integreeritud ka olulisemad ettevõtjate poolt kasutatavad erasektori e-teenused.

4. Avaliku sektori teenuspakkujate küsitlus

Käesolevas peatükis antakse ülevaade olemasolevatest pääsuhalduslahendustest, võrreldakse neid omavahel ja antakse ülevaade intervjuude käigus avaliku sektori teenusepakkujate poolt esitatud nõuetest (4.1), kirjeldatakse sobivaimat lahendust (4.3) ning võimalikke alternatiive ja tulevikulahenduse paiknevust (4.3.4).

Teenusepakkujatega viidi läbi 18 intervjuud.[5] Kahe intervjuu puhul ei õnnestunud andmeid koguda:

- Selgus, et kuna PPA kodanikule suunatud teenused seisnevad eri dokumentide taotlemises, puudub igasugune volituste kontrolli süsteem;
- Eesti Pank ja Finantsinspektsioon kasutavad nii klientide teenindamiseks kui nende pääsuhalduse juhtimiseks ühte infosüsteemi.

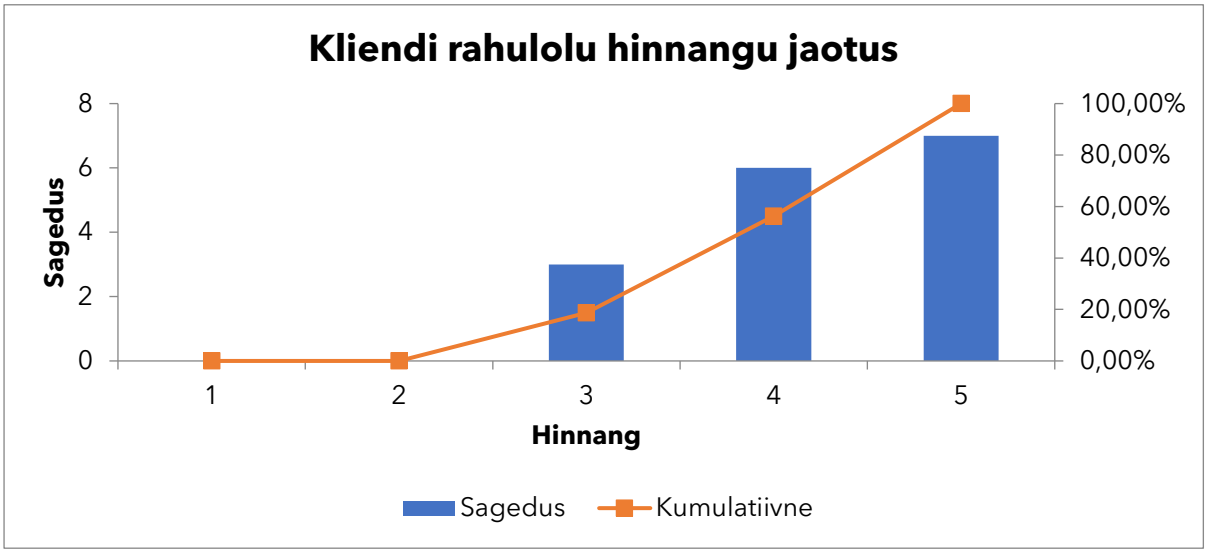
[5] Vt. Lisa 3 - Läbi viidud intervjuud.

4.1 Intervjuude leiud ja intervjueeritavate püstitatud nõuded

Juhime tähelepanu, et allpooltoodud intervjuude leiud on nummerdatud viitamise mugavuse eesmärgil. Nummerdus ja leidude järjekord ei indikeeri leidude olulisust.

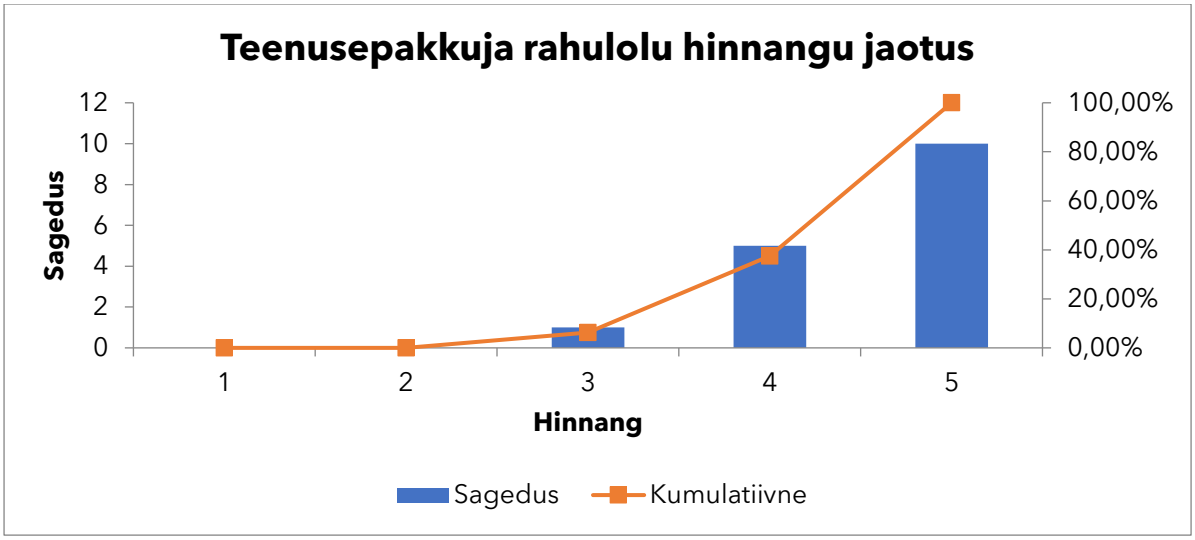
1. Pääsuhalduse süsteemide integreerituse sügavus varieerub oluliselt erinevate teenusepakkujat lõikes. Intervjueeritud teenusepakkujatest selgelt kõige keerulisem ja kõige rohkemate teenustega põimunud pääsuhalduse süsteem on realiseeritud MTA-l. Selles süsteemis jagatakse pääsuõigusi kuni üksiku deklaratsiooni või ka deklaratsioonide perioodi tasemeni (näiteks auditi puhul). Skaala teises äärmuses on PPA, kellel sisuliselt puudub vajadus pääsuhalduse lahenduse järele ning ka lahendus ise.
2. Kõige levinumad välised süsteemid, mida pääsuhaldusel kasutatakse on äriregister (78% küsitletutest; reeglina saadakse siit algne volitus, mille alusel antakse kasutajale õigus edasiseks volituste halduseks või toiminguteks). Sellele järgnevad rahvastikuregister (56%; kontrollitakse inimese olemasolu, hooldusõigust jmt rahvastikuregistris asuvaid ja pääsuõiguse juriidiliseks aluseks olevaid andmeid) ja töötamise register (17%; kontrollitakse inimese töötamist ettevõttes).
3. Eraldiseisvat pääsuõiguste jaoks mõeldud süsteemi kasutatakse pigem harva (17% juhtudest), enamasti on pääsuõigused mõnda äriinfosüsteemi sisse ehitatud. Mõne teise süsteemi käest tuuakse pääsuõigusi 39% küsitletud asutustes. See tähendab, et puudub küll eraldiseisev pääsuhalduse lahendus, kuid väiksemad infosüsteemid pärivad pääsuõiguste infot mõnelt suuremalt äriinfosüsteemilt.
4. Reeglina on asutustes kasutusel rollipõhine pääsuhaldus (78%), nimekirjapõhist pääsuhaldust on 39% ja atribuudipõhist 33% juhtudest (atribuudiks peamiselt vanus, MTA puhul ka autentimise tase). Mitmel puhul on kasutusel mitu erinevat pääsuhalduse mudelit, seda nii omavahel kombineerituna kui eri rakendustes. Paljud teenused sisaldavad äriloogikat, et teenuse osutamise lubatavust kontrollitakse teenindatava registri (alkoholiregister, ärikeeldude nimekiri vms.) või kohalikult peetavasse nimekirja alusel.
5. Enamasti, kuid mitte alati on rollide nimekiri konfigureeritav (56%)
6. Mitme organisatsiooni tuge ei paku ükski praegune pääsuhalduse lahendus.

7. Üheski asutuses ei mõõdeta kasutaja rahulolu pääsuhalduse lahendusega eraldi rahulolust tervikliku infosüsteemiga. Keskmine hinnanguline kasutaja rahulolu (mida enamasti ei mõõdeta pääsuhalduse lõikes) on 4.15 skaalal 1-5 (Joonis 1). Kasutajad on pääsuhaldusega teenusepakkujate arvates üldiselt rahul.



Joonis 1. Kliendi rahulolu hinnangu jaotus

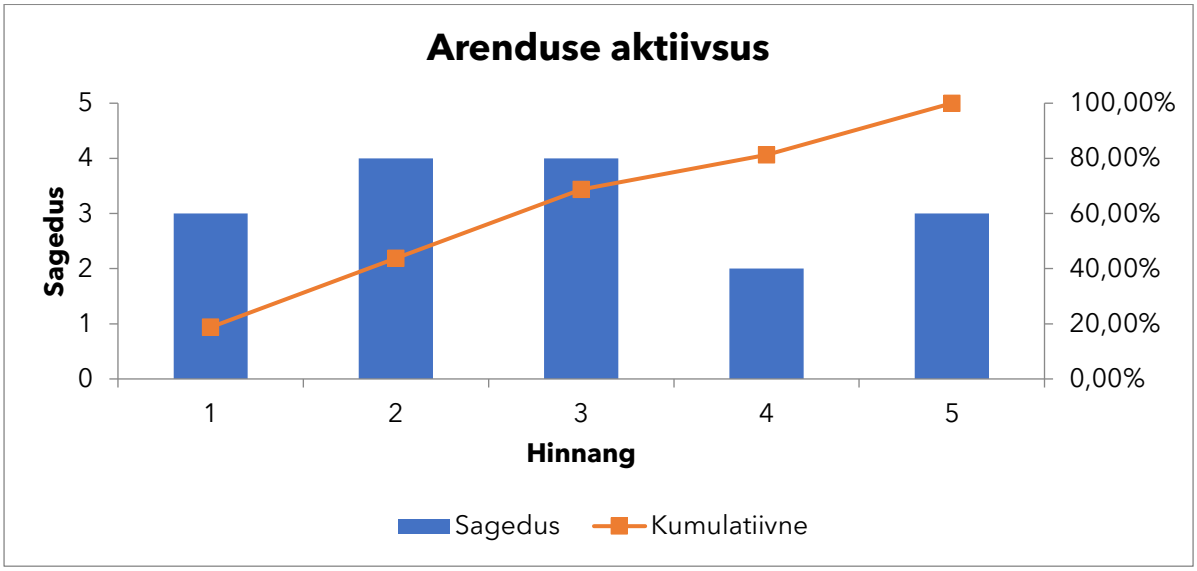
Keskmine teenusepakkuja rahulolu pääsuhalduse lahendusega on 4.57 skaalal 1-5 (Joonis 2). Seega on teenusepakkuja pääsuhalduse lahendusega üldiselt rahul ning see rahulolu on märksa suurem, kui lõppkasutaja oma.



Joonis 2. Teenusepakkuja rahulolu hinnangu jaotus

8. Intervjuude käigus uuriti ka pääsuhalduslahenduste arenduse aktiivsust mida paluti hinnata skaalal ühest viieni. Selgus, et lahendused on erineva arendusaktiivsusega

(Joonis 3). Leidus nii aktiivses arenduses olevaid kui ka täiesti passiivseid lahendusi. Konkreetset trendi tuvastada ei õnnestunud, lahenduste jaotus eri aktiivsushinnangute vahel on ühtlane.



Joonis 3. Pääsuhalduslahenduste arenduse aktiivsuse jaotus

Intervjuude läbiviimise käigus kogunes pääsuhalduse äriprotsesside ja tehniliste lahenduste kohta lisaks struktureeritud andmetele ka hulk üldisi, jagatud, tähelepanekuid.

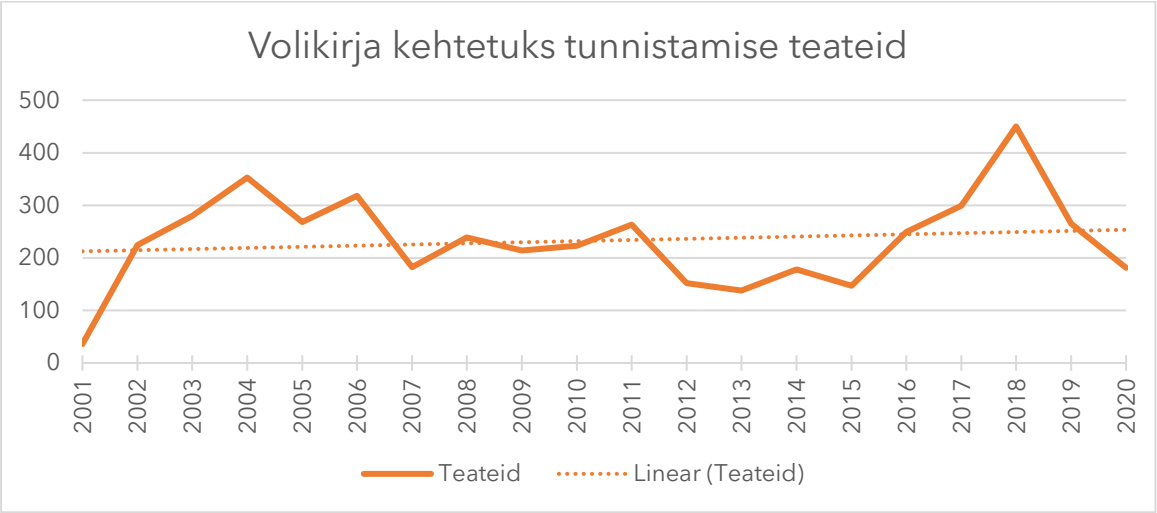
Funktsionaalsed ja sisulised väljakutsed valdkonnas on järgmised:

9. Suurimaks läbivaks funktsionaalseks probleemiks avaliku sektori teenusepakkujatele on juriidiliste isikute esindamise erindid, mis lähtuvad tsiviilseadustiku üldosa seaduse § 34 lõikest 2, mis sätestab, et juriidilise isiku ühise esindamise korral võivad juhatuse liikmed volitada üht või mitut enda hulgast teatud tehingute või teatud liiki tehingute tegemiseks. Ükski pääsuhaldussüsteemi loonud asutustest ei ole seda automatiseerinud (sh kõige keerulisema ja võimekama pääsuhaldussüsteemi loonud MTA). Osa asutusi lahendab selle probleemi manuaalse protsessiga ja väga suur hulk asutusi lihtsalt ignoreerib erisusi võimaldades teenusele ligipääsu kõigile juhatuse liikmetele. Samas ei toonud mitte ükski erindeid ignoreerivatest teenusepakkujatest välja mitte ühtegi asjakohast kliendi kaebust või sisulist probleemi.

10. Alusregistrite[6], peamiselt äriregistri ja rahvastikuregistri, käideldavus on tõsine probleem. Paljudel juhtudel peegeldatakse kas äriregistri või rahvastikuregistri koopiat asutuse juurde, et tagada vajalik käideldavus.
11. MISP2 on reaalselt kasutusel pääsuõiguste juhtimiseks (TEHIK) ja see lahendus on kohmakas.
12. Teadlikkus teenuste osas takistab valdkonna arengut:
    a. Ei teata, et äriregister väljastab masinloetavat infot esindusõiguste erindite kohta ning seetõttu peetakse võimatuks ka vastava loogika realiseerimist teenuse juures. Näiteks kui asutus usub, et äriregister ei väljasta esindusõiguste erindite infot masinloetaval kujul, ei saa nad ka kuidagi luua masinloogikat, mis aitaks erindite käitlemist automatiseerida ;
    b. On osapooli, kes RTK SAPist pääsuhalduse eesmärgil riigiasutuste töötajate nimekirju saavad (Päästeamet hoiab seal vabatahtlike päästjate infot) ja neid, kes kangesti tahaksid (Justiitsministeerium), kuid peavad seda võimatuks. Tegu on kas teadmatusega pakutavatest võimalustest või kommunikatsiooniprobleemiga RTK ja Justiitsministeeriumi vahel.
13. Strateegilist tähelepanu vajab "lihtsate volituste" probleem, mida lahendatakse asutuseti väga erinevalt. Probleem seisneb vajaduses kontrollida ja juhtida volitusi teenuse puhul, mille väärkasutuse risk on madal. Eksisteerib kaks lahendust, mõlemad asutused peavad enda oma õigeks, kuid tõenäoliselt on tarvis riigi taseme üldist otsust:
    a. Lahendus A (Statistikaamet): realiseeritud on küllalt keeruline RBAC ja ACL lähenemisi kombineeriv volituste süsteem, deklarantfirmadele väljastatakse selgelt madala turvatasemega kasutajanimesid ja paroole;
    b. Lahendus B (Päästeamet): volitusi andmeid esitada ei kontrollita üldse aga autenditud kasutajat informeeritakse valeandmete esitamise õiguslikest tagajärgedest.
14. Paljud teenusepakkujad aktsepteerivad rutiinselt notariaalseid volitusi, mida siiski tihti (täpne statistika puudub) ei kasutata. Samas käib notariaalsete volituste

[6] Alusregistreid kasutatakse läbivalt autoriteetsete allikatena kontrollimaks isiku esindusõigust.

tühistamise kontroll hetkel parema võimaluse puudumisel käsitsi Ametlike Teadaannete kaudu. Ei ole selge, kui paljudes notariaalseid volitusi aktsepteerivates asutustes selline protsess reaalselt toimib. Tihti võetakse seisukoht, et kasutaja ise peab asutust volikirja kehtetuks tunnistamisest teavitama. Notariaalse volituse kehtetuks tunnistamine on suhteliselt harv nähtus kuid kerges tõusutrendis (Joonis 4).



Joonis 4. Volikirja kehtetuks tunnistamise teadete dünaamika. Allikas: Ametlikud Teadaanded

15. Enamasti on paralleelselt elektroonilisele pääsuõiguste haldusele olemas ka paberil, telefonitsi või muul viisil toimiv pääsuhalduse protsess. Mitte-elektroonilist protsessi kasutatakse näiteks esinduse erindi korral või välismaalaste puhul, kes oma esindusõiguste tõestamiseks peavad elektroonilise registri puudumisel dokumente esitama. Telefoni teel õiguste andmist kasutatakse juhul, kui kasutajal ei ole (väidetavalt) digivõimekust. Õiguslikult pole volitusel vorminõuet ehk volituse võib anda ka suuliselt; küll aga on keeruline sel juhul tuvastada volituse andja isikusamasus.

16. Kasutatavatest identiteetidest (st. kelle suhtes pääsuõigusi hallatakse) on kõige levinumad era- ja juriidilised isikud, kuid ka siin esineb kõikumisi. Eri asutuste määratlused eraisikute suhtes on erinevad hõlmates kodanikke, mittekodanikke ja residente ning lisaks juriidilistele isikutele käsitleb intervjuu põhjal näiteks Statistikaamet ka majandusüksust (nt talud või kodumajutuse pakkujad, kes pole registreeritud juriidilised isikud ega FIEd, kuid kes on siiski aruandluskohuslased).

17. Ajalisi piiranguid pääsuõigustele esineb vähe. MTAs kasutatakse pääsuõigusi juhtimaks ligipääsu teatud perioodi toimingutele. Haigekassa kontrollib andmete viitega laekumisel teatavate õiguste olemasolu (arsti või apteekri kuulumine vastavasse nimekirja) konkreetsel ajahetkel minevikus. Siiski on tegemist erandlike juhtumitega.

Lisaks otseselt pääsuhalduse lahendusele kerkis intervjuude käigus esile **kaks ettepanekut kas pääsuhalduse või teiste lahenduste täiendamiseks**:

18. Rolle võiks saada kasutada ka muuks, kui pääsuhalduseks. Näiteks võiks ettevõte määratleda inimese ja/või meiliaadressi, kellele saadetakse ettevõttele mõeldud teateid. Sel juhul toimub lihtsalt meiliaadressi või isiku volitamine ning enne sõnumi saatmist toimub päring "kes on asutuse X suhtes rollis 'postikana'?".
19. Ettepanek Justiitsministeeriumilt: TARA osana võiks toimuda ametlike sõnumite kätte toimetamine. Sisse logimise järel, kuid enne teenusesse sisenemist, informeeritakse kasutajat ootavatest sõnumitest ja/või piiratakse edasist tegevust, kuni sõnum on läbi loetud ja vastav kinnitus antud.

Intervjuude käigus püstitati uuele lahendusele rida nõudeid. Kas ja millised neist nõuetest uues lahenduses arvesse võtta, on edasise analüüsi küsimus. Loetelu (mitte prioriteetsuse järgi) esitatud nõuetest:

1. Kui juhatuse liige või mõni muu edasivolitamise õigusega isik ei ole enam vastavas rollis, peavad tema antud õigused kehtivuse kaotama.
2. Volitused peavad olema tähtajalised.
3. Ühel või teisel viisil peab riigis korraldatud olema vähemalt järgmiste nimekirjade haldus, neisse kuulumise abil kontrollitakse või soovitakse kontrollida pääsuõigusi:
    a. Ärikeelud;
    b. Kohtutäiturid;
    c. Kohalikud omavalitsused;[7]
    d. Riigitöötajad;[8]

[7] Kuigi riigi ja kohaliku omavalitsuste register (RKOAR) osana äriregistrist eksisteerib, avaldati soovi ka eraldi KOVide nimekirja järele. Tegu võib olla eelmainitud teadlikkuse probleemiga.
[8] Vaata ka eelmainitud teadlikkuse probleemi.

e. Notarid.

4. Rollidel võiks nende haldamise lihtsustamiseks ja õiguste tuletamise võimaldamiseks eksisteerida puukujuline struktuur, kus rollidel on alam-rollid, millel omakorda võib leiduda alamrolle.
5. Pääsuõigusi kasutavate äriprotsesside lihtsustamise eesmärgil peab eksisteerima võimalus piirata rolli määratud isikute hulka. Näiteks võib eksisteerida vajadus piirata raamatupidaja rolli täitvate inimeste hulka ühe inimeseni, rohkem selle rolli täitjaid ettevõttele määrata ei saa.
6. Peab olema võimalik inimese asendamine: kui konkreetseid õigusi omanud inimene kas lahkub ettevõttest või ei ole ajutiselt võimeline oma kohustusi täitma, peab olema võimalik kõik tema õigused toimingu tegemise hetkel üle tõsta uuele inimesele.
7. Peab olema võimalus kontrollida, kas mingi volitus kehtis kindlal ajahetkel minevikus.
8. Keskne pääsuhalduse lahendus peab olema:
    a. teenusena juhitud (sealhulgas klienditugi, SLA, pidev tootearendus, turvapaigad, kogukonna juhtimine jne.); ja
    b. kõrgkäideldav, eelkõige teenuse kättesaadavuse ja vasteaja suhtes[9].
9. Peab olema võimalus digiallkirjastatud volituseks ja volituse dokumendi üles laadimiseks.
10. Seoste osapooltena peab olema võimalik määratleda ka teiste riikide poolt väljastatud identiteete juriidilistele ja füüsilistele isikutele.[10]
11. Edasivolitamine (st olukord, kus mõnda rolli täitma volitatud isik volitab järgmise isiku sama osapoole suhtes sama rolli täitma) peab olema võimalik.[11]

[9] Täpsemaid vajadusi intervjueeritavad ei väljendanud.
[10] See ei tähenda, et soovitakse võimalust autentida välismaiste vahenditega, sest volituse andmisel tuvastatakse volituse andja ja mitte volituse saaja. Näiteks võib Eesti kodanik A volitada Rootsi kodanikku B enda esindatava äriühingu nimel MTAle deklaratsioone esitama. See eeldab keskse pääsuhalduse võimekust tuvastada A isik ja MTA võimekust tuvastada B isik.
[11] Toodi konkreetne näide advokaadibüroo ja advokaadi abide kohta, kus advokaat volitab oma abisid tema nimel toimikutele ligi pääsema.

Lisaks eeltoodud nõuetele esitati ka üldisemaid soove keskse pääsuhalduse lahenduse ja pääsuhalduse kui sellise osas:

12. Mitmed osapooled, sealhulgas ka äriregistri meeskond avaldas soovi, et regulatsioonis lihtsustataks[12] juriidiliste isikute esindamise erindeid või realiseeritaks keskne lahendus, mis võimaldaks esindusõigusega isikutel ühiselt valida üks inimene neid konkreetses rollis esindama[13];
13. Võiks eksisteerida võimalus määrata ettevõttele üks juriidiline esindaja.[14]
14. Võimalus pääsuõigusi pärida ja muuta x-tee vahendusel eesmärgiga integreerida pääsuhaldus rollide lisamise ja eemaldamise näol automatiseeritud äriprotsessidesse ning võimaldada pääsuhaldust kasutada ka masin-masin suhtluseks x-tee vahendusel.
15. Võiks olla realiseeritud töötamise registri integratsioon: kui isikute vahel töösuhe lõpeb, lõpetatakse ka tema volitused ja/või saadetakse teavitus volitajale.

4.2 Täiendavad kommentaarid leidudele

1. Juriidiliste isikute esindamise erindite automatiseerimine keskse pääsuhalduse lahenduse kaudu omab väga olulist mõju tulevikulahenduse arhitektuurile ja arenduse keerukusele. Samas ei ole teenusepakkujate poolt survet seda keskselt lahendada, kuna ka praegused detsentraliseeritud lahendused ei ole automatiseerimist piisavalt tähtsaks pidanud ja soovitame automatiseerimise kesksest lahendusest välja jätta. Teenusepakkujatel jääb võimalus erindid lahendada vastavalt praegustele äriprotsessidele või automatiseerida see enda infosüsteemides. Detsentraliseeritud automatiseerimine ei välista keskse pääsuhalduselahenduse kasutamist. Võtame projekti järgmises etapis eesmärgiks kirjeldada võimalikke erindite automatiseerimise valikuid koos arhitektuurinägemusega. Koos tulevikulahenduse arhitektuuri kokkuleppimisega

[12] Näiteks võib juriidilist isikut esindada kas iga juhatuse liige, kogu juhatus tervikuna või juhatuse liikmed teatud kombinatsioonis.
[13] Erindite peamise probleemina nähakse vajadus luua väga väikese osa kasutajate jaoks keerulised äriprotsessid, mis võimaldaksid dokumentide esitamisel või kannete tegemisel koguda eri osapoolte allkirju.
[14] Sisuliselt keskselt kontrollitav volitus juriidiliste isikute vahel.

tehakse ka otsus kas ja kuidas automatiseerimine on keskse lahenduse skoopi kaasatud.

2. Alusregistrite kõrge käideldavuse tagamiseks kasutatav kohaliku koopia lahendus on tehniliselt kindlasti mõistetav, kuid kaheldava legaalsuse ning turvalisusega. Juriidilises mõttes on probleemiks alusregistrite andmete töötlemine viisidel, mis ei ole otseselt seotud kodaniku tahtega (registrite koopiaid hoitakse nii enne kui pärast teenuse osutamist). Turvalisuse osas kahekordistab iga andmebaasi koopia andmete lekkimise tõenäosust sel lihtsal põhjusel, et andmeid hoitakse ühe asemel kahes kohas ning tõhusad peavad olema kaks ja mitte üks komplekt kaitsemeetmeid. Kuna lahendus on reaalselt kasutusel, võtame projekti järgmises etapis eesmärgiks analüüsida lahenduse õiguslike aspekte ning kirjeldada asjakohaseid soovitatavaid muudatusi tulevikulahenduse kontekstis.
3. MISP2 kasutamine pääsuõiguste juhtimiseks on kohmakas, sest lahendus on algselt loodud teisel eesmärgil – x-tee teenuste ilma infosüsteemita välja kutsumise võimalus lõppkasutajale ajutise lahendusena või erijuhtumite lahendamiseks. Praeguse lahendusega ei ole seda võimalik ka palju paremaks saada. Alternatiivid on kas MISP2 mugavamaks ehitamine või vastava spetsiaalse infosüsteemi loomine. Kumb alternatiividest on otstarbekam, vajab eraldi analüüsi.
4. Vajadus pakkuda tuge ajas tagasi minevate pääsuõiguste kasutamiseks on väike ning analüüsi käigus lepiti koostöös RIA-ga kokku, et seda võimekust ei kaasata tulevikunägemuse praegusesse skoopi.
5. Ettepanek, et TARA osana võiks toimuda ametlike sõnumite kätte toimetamine otsustati RIA-ga kokkuleppel käesoleva lahenduse skoobist välja jätta.
6. Ettepanek, et rolle võiks saada kasutada ka muuks, kui pääsuhalduseks (näiteks e-posti aadressi volitamine ametlike teadaannete saajaks), otsustati RIA-ga kokkuleppel hetkel lahenduse skoobist välja jätta. Täiendava vajaduse ilmnemisel saab nõude tulevikus läbi analüüsida ja realisatsioonis arvesse võtta.
7. Intervjuude käigus esitati ka ettepanek ametnike endi pääsuhalduse küsimuste lahendamiseks, mis on antud analüüsi ja tulevikulahenduse ning seda ilmestava prototüübi skoobist väljas. Küll aga kirjeldatakse käesoleva analüüsi II etapis loodava arhitektuuridokumendi raames funktsionaalsus ja ärilised vajadused, mis on

suunatud pääsuhalduse haldamisega tegelevatele ametnikele (nt nimeruumi haldajad).

4.3 Järeldused ehk võimalikud tulevikulahendused

Käesoleva hankega on tulevikulahendusele püstitatud peamised funktsionaalsed nõudmised ja tööde kirjeldus. Lähtuvalt käesoleva hanke tööde kirjeldusest ja parimatest praktikatest läbisime sobivama tulevikulahenduse leidmiseks järgmise samm-sammulise protsessi:

Samm 1: Disainieesmärgid ja -otsused võimalike lahenduste ruumi piiramiseks;

Samm 2: Olemasoleva lahenduse keskse kasutuselevõttu hindamine;

Samm 3: Uue lahenduse väljatöötamise hindamine; ja

Samm 4: Soovitused tulevikulahenduse osas.

4.3.1 Samm 1: Disainieesmärgid ja -otsused võimalike lahenduste ruumi piiramiseks

Tulevikulahendusele on hankedokumentides püstitatud peamiselt funktsionaalsed nõuded, ennekõike vajadus määrata pääsuõigusi era- ja juriidiliste isikute vahel kõikvõimalikes kombinatsioonides. Analüüsi käigus on täiendatud arusaama ettevõtjate ja avaliku sektori teenusepakkujate ootustest tulevikulahendusele (vt p 3 ja 4).

Nii laia funktsionaalsete nõuete ulatuse realiseerimiseks on väga palju väga erinevaid võimalusi: öeldakse, et lahenduste ruum on piiramatu. See teeb aga võimatuks nii kõigi nende võimaluste seast õige valimise kui ka vastamise küsimusele, milline lahendustest on "õige"? Arhitektuuri protsessis tehakse seetõttu järgmise sammuna rida disainiotsuseid, mis lahenduste ruumi piiravad ning vähendavad oluliselt kaalutavate alternatiivide hulka.

Lähtudes käesoleva hanke tööde kirjeldusest, analüüsi käigus kogutud leidudest, riigi infosüsteemi arhitektuurist ning laiemast tehnoloogilisest kontekstist püstitati kirjeldatud tulevikulahendusele järgmised disainieesmärgid:

- **Integratsioon**. Lahendus peab olema lihtsasti integreeritav võimalikult suure hulga riigi infosüsteemi osadega vajamata nende suuremahulist muutmist ja/või ümber kirjutamist tagades lahenduse mõistliku kulubaasi;
- **Turvalisus**. Lahendus peab olema kergesti kaitstav sisaldades minimaalselt tundlikku informatsiooni ning võimaldades talletatud andmete tervikluse tagamist nii andmehulga kui terviku kui ka üksikute jagatud õiguste baasil;
- **Juurutatavus.** Lahendus peab olema juurutatav ja edaspidi hallatav vajamata suuremahulisi ümberkorraldusi ei lahendust haldavate ega seda kasutavate organisatsioonide töös eeldades minimaalse keerukusega äriprotsesse;
- **Realiseeritavus.** Nii lahendus kui selle integratsioon teda kasutavate infosüsteemidega peab olema mõistlike kuludega saadaoleva ressursi poolt realiseeritav.

Neist eesmärkidest kõige olulisem on integratsioonivõimekus. Ühest küljest tähendab see vajadust katta võimalikult suur osa klientsüsteemide poolt vajatavast funktsionaalsusest, kuid teisalt ka vajadust viia minimaalseks kasulikuks integratsiooniks vajalikud muutused infosüsteemis miinimumini. Siit tuleneb disainiotsus, et **uus lahendus peab olema suuteline toimima kliendina olemasolevatele infosüsteemidele**.

Turvalisus disainieesmärgina on kahtlemata oluline. Samas eksisteerib siin selge konflikt realiseeritavuse ja integratsiooni eesmärkidega. Kõige turvalisem oleks uus lahendus realiseerida ilma igasugust keskset taristut omamata nii, et kõikide infosüsteemide kõik pääsuõigused asuksid jätkuvalt infosüsteemides endis. Selline arhitektuur aga seaks nii funktsionaalsuse kui käideldavuse osas kõigile klientsüsteemidele sarnased ja kõrged funktsionaalsed ja mittefunktsionaalsed nõuded. Samuti oleks raskendatud pääsuõiguste ristkasutus asutuste vahel. Siit tuleb disainiotsus, et **uus lahendus peab olema suuteline minimeerima keskselt hoitavaid andmeid jättes need võimalusel klientsüsteemi hallata, kuid pakkudes ka alternatiivi.**

Organisatoorsest küljest on oluline mõista, et keskne pääsuhalduse lahendus eeldab igal juhul keskse tooteorganisatsiooni loomist, seda täiesti sõltumatult arhitektuursetest otsustest. Seega ei ole juurutatavus seotud mitte niivõrd keskse tooteorganisatsiooni loomise või selle keerukusega vaid lisanduvate äriprotsesside keerukuse minimeerimisega. Samuti on oluline, et lahendus peab olema juurutatav (ja edaspidi uuendatav) sammhaaval

eeldamata kõigi klientsüsteemide üheaegset muutust. Siit tuleb disainiotsus, et **lahendus peab olema võimalikult suurel määral hallatav klientsüsteemide haldurite poolt**, kuna organisatsiooni piire ületavad äriprotsessid on olemuslikult keerulised.

Kuna nii funktsionaalsest kontekstist, hankedokumendist kui ka läbi viidud intervjuudest selgus äärmiselt suur variatiivsus nii funktsionaalsete nõuete kui integratsioonimustrite vajaduste osas, tuleneb siit disainiotsus, et **lahendus peab olema võimalikult paindlik**.

Realiseeritavuse vaatepunktist minimeeriks uue lahenduse realisatsiooniriske ja -kulusid kõige efektiivsemalt mõne karbitoote kasutuselevõtt. Selline lahendus aga oleks selges vastuolus nii juurutatavuse kui tõenäoliselt ka turvalisuse eesmärkidega, nõudes klientsüsteemidelt kohandumist karbitoote semantiliste ja tehniliste lahendustega ning tekitades keskse rollihoidla. Küll aga on mõistlik kasutada olemasolevaid lahendusi nii suurel määral, kui see on vähegi võimalik. Näiteks ei ole ilmselt mõistlik luua ja juurutada uut turvalist kanalit klientsüsteemidega suhtlemiseks. Siit tulevad disainiotsused, et **lahendus peab tuginema mõnele olemasolevale lahendusele** ning **lahendus peab klientsüsteemidega suhtlemiseks kasutama x-teed**.

Tehtud disainiotsused kitsendavad võimalike lahenduste ruumi oluliselt.

4.3.2 Samm 2: Olemasoleva lahenduse keskse kasutuselevõttu hindamine

Vastavalt hanke tööde kirjeldusele oli üheks olemasolevate süsteemide kaardistuse uurimisküsimuseks, kas mõnda olemasolevatest lahendustest on võimalik kasutusele võtta keskse pääsuhalduse süsteemina. Vastus on, et sellist süsteemi leida ei õnnestunud.

1. Analüüsi käigus ei õnnestunud leida lahendust, mida juba kasutataks mitme eri organisatsiooni poolt.[15] Järelikult ei toeta olemasolevad süsteemid rollide eristamist organisatsioonide järgi, mis on keskse pääsuhaldussüsteemi vältimatu eeldus.
2. Reeglina ei ole pääsuhaldus üldse lahendatud lahus mõnest äriinfosüsteemist ning, kui see siiski on eraldatud, on süsteem ülimalt sõltuv konkreetsest funktsionaalsest ja tehnilisest keskkonnast. Näiteks on MTA pääsuhalduse süsteem küll äärmiselt võimekas ning realiseeritud eraldi komponendina ning tootena juhitud, kuid sõltub

[15] Erandiks on Finantsinspektsiooni ja Eesti Panga poolt jagatav lahendus, kuid seal on tegu kogu infosüsteemi omavahelise ristkasutusega. Samuti ei ole lõpuni tegu eri organisatsioonidega.

olulisel määral MTA isikute halduse lahendusest. Mis omakorda, tulenevalt MTA äriprotsessidest, on nii keeruline kui ka MTA-spetsiifiline.

MTA lahendus oleks tehniliselt võimalik kõigile disaininõuete vastama panna, olemasolev süsteem tuleb paindlikumaks ja võimekamaks muuta. Selle muudatuse realiseerimise tehniline keerukus on oma mahult võrreldav uue lahenduse loomisega. Samas tähendab olemasoleva lahenduse ringi kirjutamine, et kõiki soove ja vajadusi ei saa süsteemi disainimise käigus arvesse võtta ja tuleb paratamatult arvestada praeguse lahenduse teatavate piirangutega.

MTA lahenduse keskse kasutuselevõtu miinuseks on ka vajadus tagada mõistlik lähtekoodi haldus. Variantideks on:

- muudetud süsteem ka lähtekoodi tasemel MTA omast lahutada (see võib vajaliku funktsionaalsuse realiseerimiseks igal juhul vajalikuks osutuda); või
- luua vajalik taristu lähtekoodi jagamiseks.

Esimene variant lisab olulisel määral arendusmahtu. Teise variandi puhul ei ole selge, kui efektiivne saab olla süsteemi jagamine kahe erinevalt eesmärgistatud organisatsiooni vahel.

4.3.3 Samm 3: Uue lahenduse väljatöötamise hindamine

Vastavalt hanke tööde kirjeldusele on mõistlik kaaluda alternatiive ning analüüsida päris uue lahenduse väljatöötamise otstarbekust. Käesoleva projekti hankeprotsessis on autorid selle protsessi läbinud ning esitatud võimaliku visiooni kesksest pääsuhalduslahendusest. Üheks analüüsiküsimuseks oli, kas esitatud visioon kesksest pääsuhalduslahendusest peab jätkuvalt paika.

Keskse pääsuhalduslahenduse visioonini jõudmine

Üheks viisiks sedalaadi analüüsi alustamiseks on meetod, kus uuritakse, kuidas on antud probleemi lahendanud keegi, kellel see esineb märkimisväärselt suuremal määral.[16]

[16] Näiteks pöördusid autoinsenerid lennukiehitajate poole kui oli küsimus sellest, kuidas suuri ratastel veerevaid masinaid kiiresti pidama saada, nii jõudsid autodele ABS pidurid.

Google on kahtlemata maailma kõige suuremat ja keerulisemat infosüsteemi käitav organisatsioon. Samuti on Google oma organisatsiooni arhitektuurilt sarnane riigiga, koosnedes suurest hulgast üksteisega suhteliselt lõdvalt seotud äriüksustest, kellest igaühel on oma eelarve, mandaat, strateegia jne. 2019. aastal avaldasid Pang et al artikli Zanzibar: Google's Consistent, Global Authorization System.[17] Selles kirjeldatakse pääsuhalduste süsteemi, mis definitsiooni järgi vastab nõudele tugineda mõnele olemasolevale lahendusele, nõudele hajutatud hallatavuse kohta ning ka nõudele paindlikkusele. Seega ei ole Zanzibar kui lahendus otseselt kasutusele võetav, küll aga saab üle võtta tema üldise arhitektuurimustri, mis koosneb kesksest arvutusmootorist, mida klientsüsteemid oma vajadustele vastavalt konfigureerivad.

Lisades vastavuse teistele disainiotsustele saame uue lahenduse, mida üldjoontes[18] võib kirjeldada järgmiselt:

- Info seadustest tulenevate pääsuõiguste kohta (näiteks juhatuse liikme esindusõigus) jäävad hallatavaks nende praeguste haldurite poolt. Samuti võivad kõik klientsüsteemid, mille puhul muutus infosüsteemis ei kaalu üles kasutajamugavust[19], jätkata kõigi pääsuõiguste haldamist oma infosüsteemis, sest **uus lahendus peab olema suuteline minimeerima keskselt hoitavaid andmeid jättes need võimalusel klientsüsteemi hallata kuid pakkudes ka alternatiivi;** ning **uus lahendus peab olema suuteline toimima kliendina olemasolevatele infosüsteemidele.**
- Keskselt luuakse lahendus, mis on suuteline koondama pääsuõigusi puudutavat informatsiooni ning seda ka haldama, sest **uus lahendus peab olema suuteline minimeerima keskselt hoitavaid andmeid jättes need võimalusel klientsüsteemi hallata kuid pakkudes ka alternatiivi** ning **uus lahendus peab olema suuteline toimima kliendina olemasolevatele infosüsteemidele.**
- Keskne lahendus tugineb Zanzibari protsessimudelile, kus pääsuõigused on jagatud eri organisatsioonide hallatavateks nimeruumideks ning kus on võimalik määratleda milliseid iganes jagatavaid pääsuõigusi, sest **lahendus peab olema võimalikult**

[17] Pang, Ruoming, Ramón Cáceres, Mike Burrows, Zhifeng Chen, Pratik Dave, Nathan Germer, Alexander Golynski et al. "Zanzibar: Google's consistent, global authorization system." In 2019 {USENIX} Annual Technical Conference ({USENIX}{ATC} 19), pp. 33-46. 2019.
[18] Detailsemalt kirjeldab uut lahendust dokument "Tulevikulahenduse kirjeldus."
[19] Ehk, infosüsteemi muutus on liiga kallis, et õigustada pääsuõiguste halduse liikumist keskseseselt lahendusse.

suurel määral hallatav klientsüsteemide haldurite poolt, **lahendus peab olema võimalikult paindlik** ja **lahendus peab tuginema mõnele olemasolevale lahendusele**

- Keskne lahendus suhtleb väliste infosüsteemidega x-tee vahendusel, sest **lahendus peab klientsüsteemidega suhtlemiseks kasutama x-teed**.

Hankeprotsessis esitatud visioon kujutab oma olemuselt keskse koordinatsiooniga hajusat võrgustikku, mille eri osi käitavad eri asutused - nii alusregistrid kui klientsüsteemid on osa terviklahendusest. Seetõttu on küsimus lahenduse organisatoorsest, funktsionaalsest ja tehnilisest paiknemisest ühest küljest raskesti vastatav ja teisalt on võrgustiku keskse sõlme käitajal oluline vastutus suure hulga osapoolt ees. Intervjuudest ei selgunud, et mõni teine asutus peale Riigi Infosüsteemi Ameti võiks olla sobilik toodud visioonis koordineerivat rolli täitva keskse lahenduse organisatoorseks või tehniliseks käitamiseks, ning et eesti.ee-le võiks olla alternatiive funktsionaalse asukoha mõttes.

Käesoleva projekti hankeprotsessis esitatud visioon peab jätkuvalt paika ning on suuteline täitma kõik püstitatud nõuded. Seejuures tuleb rõhutada, et kas ja mil määral toodud nõudeid on mõistlik täita, on täiendava diskussiooni objekt.

4.3.4 Samm 4: Soovitused tulevikulahenduse osas

Autorite hinnangul näitas läbi viidud analüüs, et käesoleva projekti hankeprotsessis esitatud visioon peab jätkuvalt paika ning on suuteline täitma kõik püstitatud nõuded ja on juba visiooni tasemelt alates mõeldud toetama paljusid organisatsioone ning integratsioonimudeleid.

Samuti võimaldab praegune visioon paindlikult (st enne realisatsiooni) lisada uut funktsionaalsust ja arvesse võtta strateegilisi soove.

Autorid ei pea otstarbekaks luua täiesti uut visiooni, kuna hetkel ei ole suudetud defineerida ühtki nõuet, millele olemasolev visioon ei vastaks. Uue visiooni loomiseks peaks kogu protsess, sealhulgas käesolev analüüs uuesti otsast algama. Tarvis oleks püstitada senisest täpsemad funktsionaalsed nõuded ja seada konkreetsemad strateegilised eesmärgid, et tagada kõlbmatuks tunnistatud olemasoleva visiooni puuduste kõrvaldamise uue visiooni poolt.

5. Teenuskeskkondade kaardistus

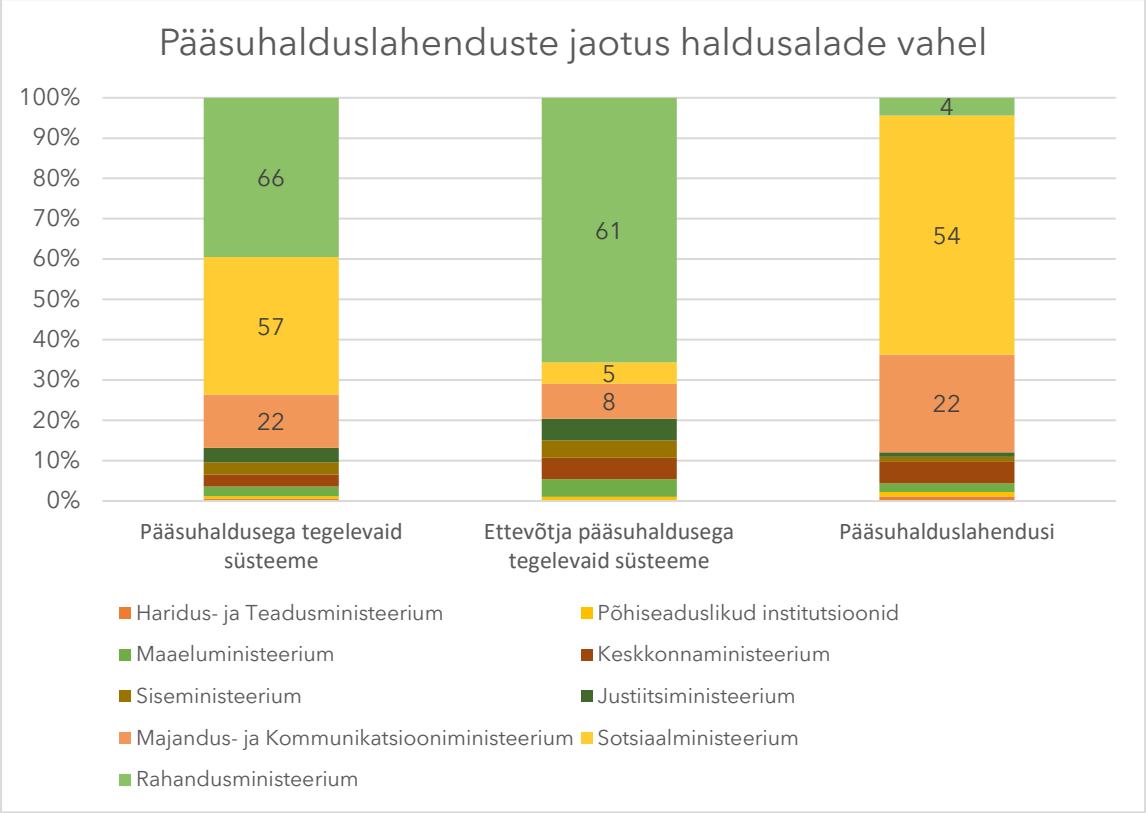
Osana läbi viidud uuringust kaardistati ka ettevõtjate poolt kasutatavad teenuskeskkonnad, kus pääsuhaldusega tegeldakse. Selleks paluti intervjueeritavatel jagada nimekirja nende halduse all olevatest vastavatest infosüsteemidest. Detailse teenuskeskkondade nimekirja koostamine põrkus olulistele väljakutsetele:

- Suur osa intervjueeritavatest sellist nimekirja kas ei omanud (sest teenuskeskkond kui selline ei ole reeglina juhtimise objekt ning teenus kui selline võib aga ei pruugi sisaldada pääsuhalduse komponenti) või ei jaganud seda;
- Teenuskeskkonna mõiste on hajus ning väga mitmeti tõlgendatav. Näiteks e-tollis on palju sisuliselt eri süsteeme, RIKi ühest keskkonnast viidatakse eri süsteemidele, millest mõnesse ei pea ja mõnesse peab uuesti sisse logima (kas tegu on ühe, kahe või kolme teenuskeskkonnaga?), Päästeametil on mitu eri süsteemi sama keskkonna sees;
- Era- ja juriidilistele isikutele mõeldud teenuste piir ei ole tingimata selge. Näiteks postipaki ja reisija deklaratsiooni rakendus on sobilikud mõlemale;
- Osa teenuskeskkondi on eri funktsioonide ja eri kasutajagruppidega aga on sisuliselt üks süsteem (nt Eesti Pank ja Finantsinspektsioon).

Kuigi täpset nimekirja koostada ei õnnestunud, oli võimalik hinnata ettevõtjate poolt kasutatavate teenuskeskkondade hulka ning (jämedalt) asutustes kasutusel olevate pääsuhalduslahenduste arvu. Kokku opereerib Eesti avalik sektor umbes 167 teenuskeskkonda, kus ühel või teisel moel tegeldakse pääsuhaldusega, neist 93 on suunatud ettevõtjale. Erinevaid pääsuhalduslahendusi on kasutusel umbes 91. Kaitseministeeriumi, Kultuuriministeeriumi ja Välisministeeriumi haldusalades käesoleva uuringu mõttes pääsuõigustega tegelevaid avalikke teenuskeskkondi leida ei õnnestunud. Kokkuvõte eri asutuste ja haldusalade poolt käitatavate teenuskeskkondade hulgast on toodud lisas 2 (Lisa 2 - Pääsuhaldusega tegelevate teenuskeskkondade hulk haldusalade lõikes).

Ettevõtja pääsuhaldusega tegelevad süsteemid jagunevad avalikus sektoris ebaühtlaselt (Joonis 5). Kõige enam on selliseid süsteeme Rahandusministeeriumi haldusalas, peamiselt käitab neid süsteeme MTA. Teisele kohale jäänud Majandus- ja Kommunikatsiooniministeerium opereerib mitmeid kordi väiksemat hulka süsteeme.

Samas, kuna MTAs ja veel mõnes suuremas asutuses on pääsuhaldus suuremal või vähemal määral konsolideeritud, siis pääsuhalduslahenduste hulga jaotus haldusalade vahel on oluliselt teistsugune. Arvestada tuleb siiski, et ka pääsuhaldusega tegeleva süsteemi määratlus ei ole täpne ning tegu on teises hinnanguga, mis tugineb esmasele teenuskeskkondade hulga hinnangule ning läbi viidud intervjuudele.



Joonis 5. Pääsuhaldusega tegelevate süsteemide jaotus haldusalade vahel[20]

[20] Täpsema info puudumisel on eeldatud, et TEHIKu kõik süsteemid omavad eraldi pääsuhaldust.

Lisa 1 - Intervjuu küsimused

- Tehnilised ja arhitektuursed küsimused
    - Kas tegu on pääsuhalduse lahenduse näol on tegu eraldiseiseva süsteemiga või osaga mõnest infosüsteemist? (JAH/EI)
    - Kas pääsuhalduse lahendus on kasutatav teiste süsteemide poolt? (JAH/EI)
    - Kas kasutatakse rollipõhist pääsuhaldust (RBAC)? (JAH/EI)
    - Kas kasutatakse tegevuste nimekirja põhist pääsuhaldust (ACL)? (JAH/EI)
    - Kas kasutatakse atribuudipõhist pääsuhaldust (ABAC)? (JAH/EI)
    - Milline on kasutaja hinnanguline rahulolu pääsuhalduse lahendusega? (1-5)
    - Milline on teenusepakkuja hinnanguline rahulolu pääsuhalduse lahendusega (1-5)
    - Kas õiguste/rollide nimekiri on konfigureeritav? (JAH/EI)
    - Milliseid välised osapooli kasutatakse pääsuõiguste määramiseks? (loend)
    - Milline on pääsuhalduse lahenduse arenduse aktiivsus skaalal? (1-5)
- Funktsionaalsed küsimused
    - Peamised head: mida uus süsteem peaks kindlasti olemasolevast lahendusest üle võtma?
    - Peamised vead: millised olemasoleva lahenduse probleemid peaks uus süsteem kindlasti lahendama?

Lisa 2 - Pääsuhaldusega tegelevate teenuskeskkondade hulk haldusalade lõikes

Haldusala	Täpsustus	Pääsu-haldusega tegelevaid süsteeme	Ettevõtja pääsu-haldusega tegelevaid süsteeme	Pääsu-haldus-lahendusi
Haridus- ja Teadusministeerium	ETIS	1	0	1
Justiitsiministeerium	Justiitsiministeerium	6	5	1
Keskkonnaministeerium	Keskkonnaministeerium	5	5	5
Maaeluministeerium	PRIA	3	3	1
Maaeluministeerium	Maaeluministeerium	1	1	1
Majandus- ja Kommunikatsiooniministeerium	Transpordiamet	15	1	15
Majandus- ja Kommunikatsiooniministeerium	MKM (MTR)	1	1	1
Majandus- ja Kommunikatsiooniministeerium	TTJA	2	2	2
Majandus- ja Kommunikatsiooniministeerium	Ehitisregister	1	1	1
Majandus- ja Kommunikatsiooniministeerium	SOLVIT	1	1	1
Majandus- ja Kommunikatsiooniministeerium	EAS	1	1	1
Majandus- ja Kommunikatsiooniministeerium	KredEx	1	1	1
Põhiseaduslikud institutsioonid	Eesti Pank/FI	1	1	1
Rahandusministeerium	MTA	63	58	1
Rahandusministeerium	Rahandusministeerium (RHR)	1	1	1
Rahandusministeerium	Statistikaamet	2	2	2
Siseministeerium	Päästeamet	5	4	1
Sotsiaalministeerium	SKA	2	0	2

Sotsiaalministeerium	Töötukassa	2	1	1
Sotsiaalministeerium	Haigekassa	2	1	0
Sotsiaalministeerium	Pensionikeskus	1	0	1
Sotsiaalministeerium	Tööinspektsioon	1	1	1
Sotsiaalministeerium	Ravimiamet	1	1	1
Sotsiaalministeerium	Terviseamet (Vee terviseohutus)	1	1	1
Sotsiaalministeerium	TEHIK	47	0	47
		167	**93**	**91**

Lisa 3 - Läbi viidud intervjuud

Nr	Asutus/Ettevõte	Kuupäev	Tüüp
1	KeMIT	06.07.2021	Avaliku sektori teenuspakkuja
2	Transpordiamet	07.07.2021	Avaliku sektori teenuspakkuja
3	RIK	07.07.2021	Avaliku sektori teenuspakkuja
4	PRIA	14.07.2021	Avaliku sektori teenuspakkuja
5	Põllumajandus- ja Toiduamet / Maaelu ministeerium	14.07.2021 / 15.07.2021	Avaliku sektori teenuspakkuja
6	SKA	16.07.2021	Avaliku sektori teenuspakkuja
7	Finantsinspektsioon	22.07.2021	Avaliku sektori teenuspakkuja
8	PPA	23.07.2021	Avaliku sektori teenuspakkuja
9	MTA ja RMIT	26.07.2021	Avaliku sektori teenuspakkuja
10	Töötukassa	27.07.2021	Avaliku sektori teenuspakkuja
11	Tarbijakaitse ja Tehnilise Järelevalve Amet, JVIS	27.07.2021	Avaliku sektori teenuspakkuja
12	Statistikaamet	28.07.2021	Avaliku sektori teenuspakkuja
13	Riigihangete register	29.07.2021	Avaliku sektori teenuspakkuja
14	Justiitsministeerium	29.07.2021	Avaliku sektori teenuspakkuja
15	TEHIK	05.08.2021	Avaliku sektori teenuspakkuja
16	Eesti Pank	17.08.2021	Avaliku sektori teenuspakkuja
17	Päästeamet	17.08.2021	Avaliku sektori teenuspakkuja
18	Haigekassa	17.08.2021	Avaliku sektori teenuspakkuja
19	Nortal AS	18.08.2021	Persoona 1
20	Columbus Eesti AS	18.08.2021	Persoona 1
21	Bauhub OÜ	17.08.2021	Persoona 1, Persoona 3
22	AB Supremia	23.08.2021	Persoona 2, Persoona 3
23	Akkadian OÜ	27.08.2021	Persoona 3
24	Accounting Partner OÜ	18.08.2021	Persoona 2, Persoona 3
25	Eesti Raamatupidajate Kogu	Suhtlus e-kirja teel	
26	Notarikandidaat Katrin Sepp	02.09.2021	