PROUD ENGINEERS

Keskne volituste, rollide ja pääsuõiguste haldamise süsteem

Lühikokkuvõte

Koostaja: Proud Engineers OÜ

Versioon: 1.1

Kuupäev: 30.12.2021

Proud Engineers OÜ | Kristjani tee 4, 74015 Miiduranna, Estonia

getstarted@proudengineers.ee | proudengineers.ee

1. Sissejuhatus

Majandus- ja Kommunikatsiooniministeeriumi tellimusel valmis 2020.a ettevõtja ühtse veebipõhise kontaktpunkti tulevikuvaade koos arendus- ja tegevusplaaniga (teekaart), ettevõtjate sündmusteenuste arendamise analüüsi ning kontaktpunkti prototüübiga.[1] Peamiste murekohtadena toodi visioonis 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 Riigi Infosüsteemi Amet 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.

Käesolev dokument võtab kokku olulisemad projekti käigus valminud tulemid.

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

2. Hetkeolukorra kaardistus ja analüüs

Hetkeolukorra kaardistamiseks viidi läbi intervjuud avaliku sektori teenusepakkujate ning ettevõtjatega. Intervjuude eesmärgiks oli mõista:

- mis on ettevõtjate peamised vajadused ja probleemid seoses pääsuhaldusega;
- missuguseid olemasolevaid pääsuhalduslahendusi kasutatakse avaliku sektori teenusepakkujate poolt;
- missugused teenuskeskkonnad kasutavad pääsuhalduslahendusi;
- milline on sobivaim lahendus edasiliikumiseks.

Ettevõtjatega läbi viidud intervjuudest leiti, et 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, mitte niivõrd pääsuhaldusega seotud küsimustele.

Avaliku sektori teenusepakkujatega läbi viidud intervjuudest leiti, et reeglina kasutatakse rollipõhist pääsuhaldust (*role-based access control*, RBAC) ning pääsuhalduse lahendus on olemasoleva lahenduse osa, mitte eraldi liidestatud toode või teenus. Tööde käigus ei leitud olemasolevat lahendust, mida oleks võimalik keskse pääsuhalduse süsteemina kasutusele võtta, kuna ühtegi lahendust ei kasutata mitme eri organisatsiooni poolt ning see ei ole lahutatav olemasolevast äriinfosüsteemist. Seetõttu leiti, et mõistlik on edasi liikuda Proud Engineers OÜ poolt pakutud tulevikulahenduse visiooniga, mille idee põhineb Google Zanzibar'il, kuid mis on kohandatud Eesti riigi infosüsteemi nõuete ja vajadustega.

Töö käigus ei õnnestunud välja selgitada täpset pääsuhalduse lahendusi kasutatavate teenuskeskkondade nimekirja. Analüüs leidis, et 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 90.

Vaata lisaks: Hetkeolukorra kaardistus ja analüüs (PDF)

3. Tulevikulahendus

3.1. Tulevikulahenduse kirjeldus

Tulevikulahenduse kohaselt on riigi keskse pääsuhalduslahenduse ülesandeks võimaldada kasutajal keskset kontrolli tema poolt või talle antud pääsuõiguste üle terves riigi infosüsteemis. Pakutud tulevikulahenduse näol on tegemist rollipõhise pääsuhalduse lahendusega, mille keskseks mõisteks on roll või "kolmik". Viimane nimetus tuleb asjaolust, et roll on alati määratletud kolme elemendiga:

- Objekt (A), mille suhtes roll on määratud (nt „OÜ 123“),
- Roll ehk seos (X), mida määratakse (nt „juhatuse liige“); ja
- Subjekt (B), millel on objekti A suhtes roll X (nt Peeter Paan).

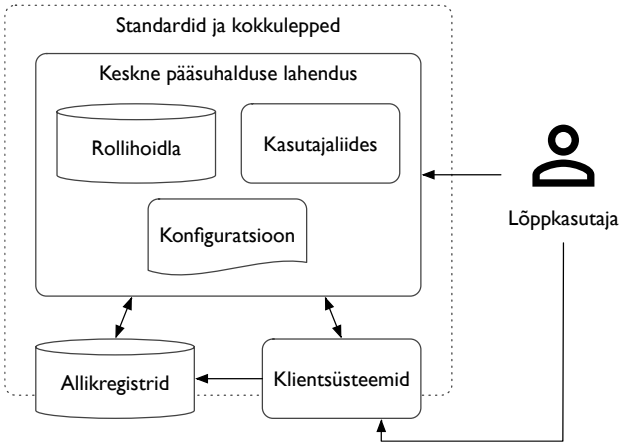
Kolmikute puhul saab kasutada kirjaviisi „A:X:B“, mida tuleks lugeda kui Peeter Paan on OÜ 123 juhatuse liige.

Tulevikulahendus koosneb neljast olulisest kontseptuaalsetest komponendist, mis kõik koosnevad tehnilisest (standardid, tarkvara, liidesed ja nende dokumentatsioon, jne) ja organisatoorsest aspektist (protsessid standardite ja tarkvara haldamiseks, liideste dokumentatsiooni ajakohastamine, kokkulepped rollide detailsusastme üle jne.). Käesolevas dokumendis kirjeldatakse ainult süsteemi tehnilist poolt ja sellest tulenevaid nõudeid organisatoorsele süsteemi aspektile.

Pakutava lahenduse neli peamist komponenti on:

- **Standardid ja kokkulepped**, mis sätestavad standardse viisi väljastada ja tarbida pääsuõigusi ning olemite seoseid üldisemalt puudutavat informatsiooni ning tagavad osapoolte sujuva koosvõime
- **Keskne pääsuhalduslahendus**, mis ühena paljudest osapooltest realiseerib standardeid, pakub keskset kasutajaliidest ning võib pakkuda keerukamat funktsionaalsust nagu teavitused, rollide omavaheliste sõltuvuste arvestamine jms
- **Standardite realisatsioonid teiste infosüsteemide juures**, mis teevad keskse pääsuhalduse lõppkasutajale läbi oma äriloogika realisatsiooni funktsionaalses mõttes kättesaadavaks
- **Pääsuhalduse konfiguratsioon**, mis kirjeldab süsteemis kui tervikus eksisteerivad rollid ning identiteedid ning nende omavahelised seosed

Tulevikulahenduse kõrge taseme visioon ja peamised komponendid on kujutatud alloleval joonisel.



Tulevikulahenduse skoobis on reaalajaline rollipõhise pääsuhalduse lahendamine isikutele, kellele Eesti avalik sektor pakub teenust seaduse või määruse ja mitte lepingu alusel. Tulevikulahenduse skoobis ei ole:

a) identiteetide (juriidilised ja eraisikud ning igasugused muud olemid, millega on isikutel võimalik seoseid omada) väljastamine ning elutsükli juhtimine, sh kasutajate tuvastamine;
b) volitamine esindusõiguse erindite korral, kus mitu ühiselt esindusõigust omavat isikut väljendavad ühiselt tahet rolli määramiseks;
c) vastamine päringutele rollide kehtivuse kohta minevikus; ja
d) mitteavalike rollide määramine.

Vaata lisaks: Tulevikulahenduse kirjeldus (PDF)

3.2. Tulevikulahenduse arhitektuur

Pääsuhalduse lahendus kui süsteem hõlmab (ning vajab toimimiseks) keskset pääsuhalduse lahendust, allikregistreid (ehk juriidilise tähendusega volituste info allikaid) ja klientsüsteeme (ehk keskse pääsuhalduse lahenduse pakutavate teenuste tarbijaid).

Nii keskse pääsuhalduse lahenduse jaoks loodud arhitektuur kui ka realiseeritav funktsionaalsus muudavad lahenduse infoturbe mõttes äärmiselt tundlikuks. Ühest küljest sisaldab ta tehnilistel põhjustel sisuliselt kogu koopiat äriregistri ja rahvastikuregistri hetkeseisust ja teisalt võib tema mittetoimimine või väärkasutus eeldatava kõrge integreerituse tõttu mõjutada kogu riigi infosüsteemi. Tegu on kesksete lahenduste puhul vältimatu seosega, kus kõrge lahenduse kasutatavus tõstab nõudeid lahenduse käideldavusele muutes samal ajal lahendust vähemkäideldavaks ning seega viies alla kasutatavust. Liiatigi on kirjeldatud lahendus komponentide mõttes küllalt keeruline. Seejuures on enamus keerukust keskendunud oraakli, rollihalduri ja vastavate liideste ümber, sest siin toimub süsteemi funktsionaalsuse, turvalisuse ja käideldavuse osas kriitiline vastamine küsimusele "kas isikul A on isiku B suhtes roll x"?

Pääsuhalduse terviksüsteemi kõrge hajususe tõttu on kesksel pääsuhalduse lahendusel suur hulk liideseid, nende toimimine ja mõistlik juhtimine on süsteemi kui terviku toimimise perspektiivist hädavajalik. See aga ei ole võimalik ilma tugeva organisatoorse taristuta, seda nii keskse lahenduse kui ka liidestatud süsteemide poolt.

Keskne pääsuhalduse lahendus vajab tugevat organisatoorset taristut toetamaks suurt hulka töökindlalt toimivaid tugiprotsesse, ilma milleta lahendus funktsionaalseid ja mittefunktsionaalseid nõudeid täita ei suuda. Alates infoturbest ja klienditoest kuni lokaliseerimiseni eeldab keeruka lahenduse käitamine mitmesuguste äriprotsesside sujuvat läbi viimist.

Keskne pääsuhalduse lahendus on tehnilise taristu mõttes mõeldud toimima pilvetaristul, infoturbe kaalutlustel tõenäoliselt pigem privaatsel kui avalikul. Vajalikud andmehoidlad ja ka süsteem ise on pigem kõrge lugemis- kui kirjutamisintensiivsusega ning tänapäeva mastaapides andmemahult pigem keskmise suurusega. Seega on lahenduse skaleerimisel selle realisatsiooni disaini faasis peamine fookus koormuse efektiivsel jaotamisel komponendiinstantside vahel. Samuti on kriitilise tähtsusega süsteemi efektiivne eraldamine liidestatud süsteemide dünaamilisest keerukusest: ka suhteliselt harvad tõrked suures hulgas süsteemides annavad kombinatsioonis väga tugeva mõju nendega liidestatud keskse pääsuhalduse lahenduse käideldavusele.

Vaata lisaks: Tulevikulahenduse arhitektuur (PDF)

3.3. Tulevikulahenduse kasutuslood ja prototüüp

Keskse pääsuhalduse lahenduse funktsionaalsus jaguneb kaheks:

- primaarsed kasutuslood, milleta ei ole võimalik süsteemi funktsiooni täita; ning
- sekundaarsed kasutuslood, mis realiseerivad toetavaid või kasutajate konkreetseid vajadusi rahuldavaid nõudeid.

Peamiste kasutuslugude visualiseerimiseks on projekti käigus loodud prototüüp, mis on kohandatud sobivaks nii arvuti kui mobiilsete seadmete ekraanile.

Keskse pääsuhalduse lahenduse prototüüp koosneb:

- **rollide ülevaate lehest**, kus on toodud loetelu kõikidest rollidest, mida pääsuhalduse lahenduse kaudu anda saab;
- **volituste avalehest**, kus on toodud ülevaade konkreetse isiku volitustest (nii talle antud kui ka tema poolt teistele antud volitused), ning
- **detailvaate modaalaknast**, kus on toodud ühe esindaja või esindatava volituste ülevaade suhtes isikuga ning kus toimub volituste haldamine.

Prototüüp on üles ehitatud põhimõttel, et see asub eesti.ee veebirakenduse sees ja seetõttu järgib uue eesti.ee disainipõhimõtteid.

Prototüübis teostatud lahenduse kasutajamugavuse hindamiseks läbi viidud kasutajatestimine tuvastas, et kasutajad peavad prototüübis esitatud lahendusi lihtsasti või väga lihtsasti kasutatavaks.

Oluline on märkida, et lahenduse kasutuskogemust mõjutab oluliselt see, kui selged ja arusaadavad hakkavad olema rolli nimetused ning kirjeldused (rolli sisu ning see, mis õigused roll annab või ei anna). Väga hea kasutuskogemuse saavutamiseks peavad nimed ja kirjeldused olema selged ning pigem põhjalikud ja detailsed.

Vaata lisaks: Kasutuslugude ja prototüübi kirjeldus (PDF), Pääsuhalduse prototüüp (brauseris vaadeldav) (ZIP), Pääsuhalduse prototüüp (kood) (ZIP)

3.4. Õiguslik analüüs

Õigusanalüüsist selgus, et ettevõtjad, kelle huvides keskset pääsuõiguste haldamise lahendust luuakse, ei näe pääsuõiguste küsimust õiguslikust vaatenurgast väljakutsena. Teenusepakkujad aga, kes avalikke e-teenuseid pakuvad, tuvastasid peamise väljakutsena

ühise esindusõiguse juhtumid olukorras, kus juriidilist isikut esindab kombinatsioon juhatuse liikmeid.

Õiguslikust vaatenurgast analüüsiti kehtivat õigust ning leiti, et puuduvad piirangud tulevikulahenduses kirjeldatud lahenduse loomiseks. Kuigi avaliku sektori teenusepakkujad viitasid intervjuudes, et esindusõiguse erandite küsimus vajaks muutmist, siis töö käigus sai selgeks, et ühise esindusõiguse eranditena on käsitletav üksnes 2,5 protsenti esindusõiguse juhtumitest, mis on osakaalult väike osa. Samuti on teenusepakkujal endal võimalik luua protsess, et ühise esindusõiguse erandite tõlgendamise asemel määraksid juriidilised isikud ise ainuesindaja teenusepakkuja süsteemis ning seda teavet oleks võimalik vahendada tulevikulahenduse süsteemi. Mitmed väljakutsed nagu notariaalsete volikirjade reaalajaline kehtivuse kontrollimine või hooldusõiguse ja eestkoste andmete väljastamise kvaliteet ja vorm, mida analüüsis käsitletakse, on pääsuhaldusega külgnevad teemad ning vajavad tähelepanu väljaspool lahendust.

Tulevikulahenduse enda reguleerimiseks nähti analüüsis ette kolm võimalust – eesti.ee määruse muutmine, keskse pääsuhalduse süsteemi vabatahtliku toetava süsteemina käsitlemine või kohustusliku kindlustava süsteemina käsitlemine. Teise või kolmanda valiku korral tuleks luua eraldi toetava või kindlustava süsteemi määrus ning kaaluda lisaks eraldi andmekogu määruse loomist. Analüüs ei tee poliitikakujundaja eest valikut, vaid kirjeldab kolme alternatiivi plusse ja miinuseid.

Vaata lisaks: Õiguslik analüüs (PDF)

3.5. Riskianalüüs

Keskse pääsuhalduse lahenduse riskianalüüs leidis kolm peamist ohtu, mis vastavad kolmele infoturbe komponendile: lahendus kas ei toimi vastavalt nõuetele, väljastab ebakorrektset informatsiooni või kaob kontroll lahenduses töödeldavate andmete üle. Kõik ohud seoti Eesti infoturbestandardi (E-ITS) kataloogi alusohtudega ning leiti riskid, mille realiseerumisel oht tekib. Enamik leitud riskidest klassifitseerus keskmiseks, enamasti on riskide realiseerumise tõenäosus madal, kuid nende potentsiaalne mõju eksistentsiaalse iseloomuga. Siiski leidub ka suuri ohte. Tuvastatud riskide maandamiseks koostati osalt E-ITS kataloogile tuginedes vajalike meetmete nimekiri, enamik meetmeid maandab mitmeid riske. Seejuures sõltub suure osa meetmete detailne realisatsioon infosüsteemi ning seda

ümbritseva protsessitaristu realisatsioonist ning arhitektuuri faasis on võimalik vaid meetmete grupi määratlemine.

Vaata lisaks: Riskianalüüs (PDF)

3.6. Arendus- ja halduskulude prognoos

Analüüsi käigus hinnati kirjeldatud süsteemi ehitamise ja käitamise võimalikke kulusid. Arvutuskäik tugineb kahele olulisele sambale: raha kulutamine on ressursimahukas vajades tellijapoolset panust tööjõu näol ning tarkvara tuleb selle toimimise tagamiseks perioodiliselt uuesti luua.

Kulude hinnangu juures on olulised saadud suurusjärgud ja mitte niivõrd täpsed numbrid, sest mitmete kululiikide puhul (näiteks kasutajale pääsuõiguste muutumise kohta saadetavate sõnumite edastamise kulu) on nende täpne hindamine keeruline. Seejuures moodustavad nii haldus- kui arenduskuludest märkimisväärse osa tellijapoolsed personalikulud, seda nii kulutuste efektiivsuse tagamise kui ka lahendust toetavate protsesside käitamise kulud.

Lahenduse käitamiseks vajalikud halduskulud sõltuvad olulisel määral algsest investeeringust, sest seda suuremad on loodud süsteemi adekvaatselt toimivana hoidmiseks vajalikud arenduskulud ning järelikult ka nende kulutuste tegemiseks vajalik personalikulu.

Kuna tegemist on keerulise paljudest komponentidest koosneva ning suure hulga liideste ning tugiprotsessidega süsteemiga, tuleb silmas pidada teiseseid kulusid, mis on käesoleva mudeli skoobist väljas: organisatsiooni keerukuse kasvust tekkinud kulud, lisandunud meeskonnaliikmete juhtimiseks, majutamiseks ning teenindamiseks tehtavad kulud, liideste kulud jne. Neid on väga raske prognoosida ning seda olulisem on nende jälgimine ning süsteemne vähendamine süsteemi realiseerimise ning käitamise ajal

Analüüs leidis, et arenduskulud jäävad vahemikku 1 112 000 eurot kuni 2 204 000 eurot ning halduskulud vahemikku 590 000 eurot kuni 1 559 000 eurot aastas.

Vaata lisaks: Arendus- ja halduskulude prognoos (PDF)

Projekti käigus valminud tulemite visuaalne esitlus