PROUD ENGINEERS

Keskne volituste, rollide ja pääsuõiguste haldamise süsteem

Tulevikulahenduse kirjeldus

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

Sisukord

1. Sissejuhatus

Käesolevas dokumendis kirjeldatakse keskse volituste, rollide ja pääsuõiguste haldamise süsteemi tulevikulahenduse visiooni. Visiooni on valideeritud intervjuude kaudu nii klientsüsteemide operaatorite kui eri rollides teenusepakkujatega.

Dokumendi eesmärgiks on kirjeldada tulevikulahendust, selle funktsionaalsust ja potentsiaalse tehnilise lahenduse mõningaid aspekte. Samuti kirjeldatakse, kuidas pakutav süsteem käituks intervjuude käigus ilmnenud keerukamate funktsionaalsete olukordade puhul. Määratlemaks süsteemi funktsionaalset ulatust võimalikult täpselt, tuuakse ära ka mittetoetatud funktsionaalsed nõuded.

2. Visioon

2.1. Ülevaade

Riigi keskse pääsuhalduslahenduse ülesandeks on võimaldada kasutajal keskset kontrolli tema poolt või talle antud pääsuõiguste üle terves riigi infosüsteemis. Seejuures tuleneb lahenduse keerukus eelkõige vajadusest täita paljude kasutajatele eri keerukusastmega funktsionaalsust pakkuvate ning eri arengu ning projekti faasides asuvate organisatsioonide vajadusi.

Sedalaadi ülesannete lahendamiseks on levinud kataloogiteenused, mis seovad identiteediga (tüüpiliselt kasutajanimi) rea rolle ning võimaldavad erinevaid töö- ja integratsioonivoogusid nende rollide juhtimiseks. Sellise kataloogilahenduse võib üles ehitada kesksena või födereeritult. Esimesel juhul on lahendus väga piiratud liidestusmudelite osas, sest keskne lahendus on olemuslikult ainus tõe allikas. Seetõttu peab kogu pääsuõigustealane info riigis asuma keskses kataloogis ning saama sealt päritud. On võimalik ka födereeritud mudel, kus pääsuhalduse infot hoitakse hulgas erinevates kataloogiteenustes, mis on omavahel kindlate reeglite alusel liidestatud. Siin on reeglina probleemiks semantiline (st. kokkulepped eri asutuses määratletud rollide tähenduse üle) ning ka tehniline koosvõime.

Visioonis püstitatud funktsionaalsuse pakkumiseks näeme ette pikka aega edukalt kasutusel olnud rollipõhise pääsuhalduslahenduse Google Zanzibar[1] arhitektuurset mudelit, mida on vastavalt Eesti kontekstile täiendatud allikregistrite mõistega. Mudeli eeliseks on ennekõike tema tõestatud toimimine suure hulga nõrgalt seotud ja funktsionaalselt erinevate infosüsteemide jagatud lahendusena. Sel viisil lahendatud pääsuhalduse süsteemist võib mõelda kui keskselt toetatud võrgustikust: kõigil võrgu sõlmedel on suur vabadus üksteisega standardsel viisil erisugust rolle puudutavat infot vahetada, kuid eksisteerib ka teatud garanteeritud omadustega keskne konfiguratsiooni ja funktsionaalsuse allikas keskse pääsuhalduse lahenduse näol.

Kaalumisel olnud alternatiivsed lahendused on toodud järgnevas tabelis.

	Kirjeldus	**Head**	**Vead**
Keskne kataloogiteenus	Keskselt paigaldatud autoriteetne allikas konkreetsete kasutajate õiguste suhtes	Lihtne realisatsioon, puudub vajadus tarkvara arendamiseks	Keeruline integratsioon baasregistritega Sisuliselt ainult üks integratsioonimudel (täielik kohaliku kataloogiteenuse asendamine)
Födereeritud kataloogiteenus	Kogum kesksest kataloogiteenusest, millega on födereeritud asutuste kohalikud kataloogiteenused	Lihtne keskse lahenduse realisatsioon, puudub vajadus tarkvara arendamiseks Võimalikud erinevad integratsioonimudelid	Vajadus kolida kõigi asutuste pääsuhaldus ühilduvale kataloogiplatvormile Piiratud hulk integratsioonimudeleid Keeruline semantiline koosvõime
Keskse toega võrgustik	Pääsuhalduse infot jagav võrgustik, mida koordineerib ja hoiab koos keskne lahendus	Paindlikud integratsioonimudelid Vastab täpselt vajadustele Vastab riigi hajusa organisatsiooni mudelile	Keerukas eritarkvara vajav lahendus

[1] 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.

Pakutud lahenduse näol on tegu rollipõhise pääsuhalduse lahendusega, mille keskseks mõisteks ongi roll või "kolmik". Viimane nimetus tuleb asjaolust, et roll on alati määratletud kolme elemendiga:

- **Objekt**, mille suhtes roll on määratud (A, näiteks OÜ 123)
- **Roll**, ehk **seos**, mida määratakse (X, näiteks "juhatuse liige")
- **Subjekt**, millel on objekti A suhtes roll X (B, näiteks Peeter Paan)

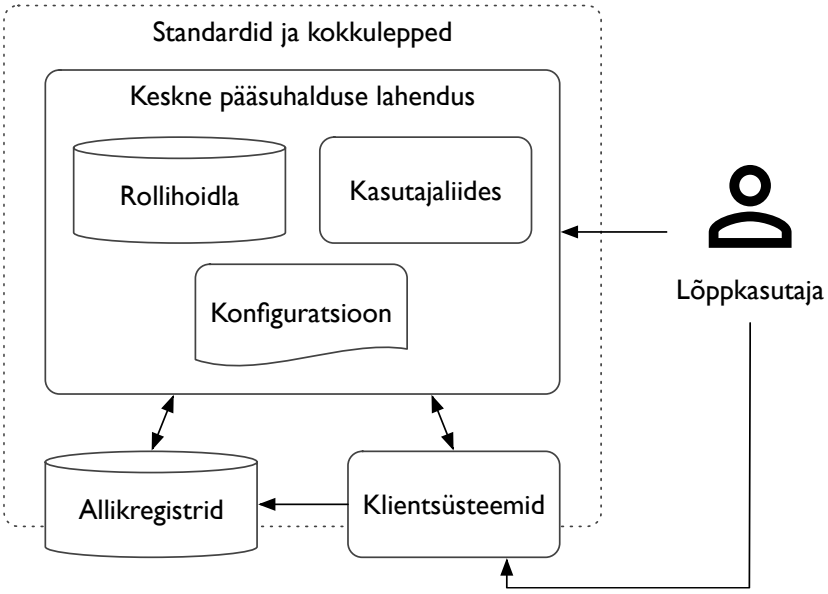
Järgnevas kasutatakse kolmikute puhul kirjaviisi "A:X:B" (loe: Peeter Paan on OÜ 123 juhatuse liige).

Ette nähtav lahendus 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 neist 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

Järgnev joonis kirjeldab süsteemi kõrge taseme visiooni peamisi komponente:



2.2. Standardid ja kokkulepped

Süsteemi aluseks on järgmised standardsed liidesed infosüsteemide vahel:

- Liides seoste pärimiseks, mis vastab küsimustele:
  - kas süsteemis eksisteerib konkreetne kolmik;
  - milliste identiteetidega on konkreetsel identiteedil konkreetne seos;
  - millised konkreetse nimega seosed eksisteerivad.
- Liides seoste muutmiseks ja kustutamiseks;
- Liides identiteetide lahendamiseks inim-loetavateks nimedeks;
- Liides keskse lahenduse konfiguratsiooni muutmiseks ja vaatamiseks.

Kõiki liideseid võivad, kuid ei pea pakkuma eri infosüsteemid, sealhulgas keskne pääsuhalduse lahendus.

Kuna kõik neli liidest on funktsionaalselt sõltumatud ning neid pakuvad süsteemis eri rolle täitvad infosüsteemid, on mõistlik neid standardeid juhtida üksteisest sõltumatult kasutades küll eelistatult samu baaslahendusi ning terminoloogiat. Järgnevas eeldatakse, et kõiki

liideseid pakutakse x-tee vahendusel ning seega loetakse nende turvamine ning tehniline standardimine lahendatuks[2].

Kõik standardid vajavad konkreetset omanikku ning peavad olema toetatud elutsükliprotsessidest (versioneerimine, pidev tagasisidestatud arendus, klienditugi, kogukonna juhtimine jne).

Kokkulepetena peab süsteemi toetama vähemalt :

- asutuste omavaheline rollijaotus, mis on oluline tagamaks süsteemi kommunikatsioonimudeli vastavust tehnilisele arhitektuurile[3] ning tagamaks süsteemi kriitiliste osade koosvõime;
- jagatud arusaam mõistlikust rollide granulaarsusest, on oluline tagamaks kasutajale võimalikult sujuv kasutajakogemus;
- jagatud arusaam süsteemi eri osapoolte käideldavusest ning käitumisest rikete puhul.

2.3. Keskne lahendus

Keskne lahendus realiseerib liidesed seoste pärimiseks ning pakub lõppkasutajale funktsionaalsust keskses rollihoidlas käideldavate rollide vaatamiseks, lisamiseks ja muutmiseks.

Olemuslikult on keskne lahendus infoturbe mõttes haavatav. Ühest küljest võimaldab edukas rünne keskse pääsuhalduse süsteemi vastu volitamata ligipääsu kõigile riigi infosüsteemis hoitavatele andmetele ja pakutavatele teenustele. Teisalt on infosüsteemid reeglina loodud tõrke korral ohutult käituma, takistades lõppkasutajale mistahes teenuste kasutamise, kuni tema vastavaid õigusi ei ole võimalik kontrollida. Seega tähendab keskse pääsuhaldussüsteemi rike kõigi temast sõltuvate infosüsteemide riket.

Järelikult peab keskne pääsuhalduse lahenduse olema realiseeritud kõrgkäideldavalt. Seda nii kättesaadavuse (mitu protsenti päringutest peab saama vastuse), garanteeritud vasteaja, plaanitava taasteaja, andmete tervikluse kui andmekao mõttes. Seejuures peab keskne

[2] Muu hulgas ka konfiguratsiooni muutmist võimaldava liidese puhul vajalik eitamiskindlus.
[3] Hajusa arhitektuuriga süsteemi ei saa tsentraliseeritult juhtida.

lahendus alati ohutult tõrkuma: kõik tehnilised tõrked, mis võivad kahtluse või tõrke korral[4] viia "jah" vastuseni ligipääsu lubamise osas peavad viima "ei tea" vastuseni.

Samuti peab sellisel tasemel tundlikkusega süsteem olema juhitud tootena koos kaasnevate protsessidega nagu turvaintsidentide jälgimine ning vaste, pidev tootearendus, kliendisuhtlus, kliendi- ja lõppkasutaja tugi, teenustaseme lepingud jne.

Pääsuõiguste haldus on funktsionaalselt nii keeruline kui kriitiline, kasutaja peab suutma mõista oma otsuste tõsiseid tagajärgi. Seejuures on pääsuhalduslahenduse keerukus sõltuvuses jagatavate rollide arvust, suure hulga omavahel sõltuvate rollide juhtimine muutub kergesti lõppkasutajale hoomamatuks. Kuna keskse lahenduse puhul suureneb käsitletavate rollide arv eri infosüsteemidega liidestumise kaudu hüppeliselt, on oluline, et keskne pääsuhalduslahenduse kasutajakogemus oleks hästi läbi mõeldud[5].

2.4. Infosüsteemide tugi

Pakutav lahendus on oma olemuselt hajus võimaldades suurt hulka eri integratsioonimudeleid. Seetõttu on süsteemi eri riigi infosüsteemi osadesse paigaldatud integratsioonipunktid olulised osad süsteemist.

Kõige kriitilisemat rolli mängivad allikregistrid[6], kelle ülesanne on jagada õiguslikult või funktsionaalselt autoriteetset infot seoste kohta. Näiteks, vaid äriregister on võimeline väljastama pädevat infot seose juhatuse liikme rolli kohta. Selliste seoste juhtimine ei saa olemuslikult olla tsentraliseeritud ning vastavat infot sisaldavate registrite võime standardse kõrgkäideldava liidese kaudu vastavat infot väljastada on seega kriitiline.

Olulised on ka liidestuspunktid, mida realiseerivad pääsuhalduse teenuseid tarbivad klientsüsteemid. Kuigi keskse pääsuhalduslahendus on planeeritud kõrgkäideldavaks, peavad klientsüsteemide liidestuspunktid olema suutelised ohutult ja kontrollitult reageerima nii kõikumistele liidestatud süsteemide vasteaegades kui kättesaadavuses.

---

[4] Näiteks alliksüsteemide kättesaadavusprobleemide või ka näiteks vahemälu roiskumiseni viinud süsteemi sisemise rikke korral.
[5] Siiski ei ole ebamõistlikku rollide hulka ja/või granulaarsust võimalik kasutajale mõistetavaks teha. Seetõttu on oluline, et kasutajakogemust toetaksid tugevad kokkulepped (vt p 2.2).
[6] Vt p 4.2.

2.5. Konfiguratsioon

Ei ole mõeldav lahendus, kus riigi infosüsteemi kesksel pääsuhalduslahendusel on fikseeritud hulk kindlate omadustega rolle. Veelgi enam, kuna rolle kasutavat äriloogikat kontrollivad oma mandaadi alusel erinevad riigiasutused, peab ka süsteemi konfiguratsioon olema juhitav erinevate riigiasutuste poolt.

Pakutavas lahenduses on pääsuõiguste konfiguratsioon jagatud nimeruumidesse, millest igaüht kontrollib konkreetne asutus. Nimeruumid võivad, kuid ei pea vastama asutustele, kuid tõenäoliselt on mõistlik eritüübiliste rollide koondamine ühtsetesse nimeruumidesse ("finants", "aruandlus", "sotsiaalvaldkond").

Nimeruumide hulka ning vastutusi nende eest võib süsteemi opereerimise käigus muuta. Siiski on tegu nii kasutajamugavuse kui teenusepakkujate arendusmugavuse seisukohalt olulise otsusega, mis vajab hoolikat kaalumist ning tõenäoliselt ka võimet kiiresti muudatusi läbi viia.

3. Funktsionaalsus

3.1. Skoop

Pakutava lahenduse skoobis on reaalajaline rollipõhise pääsuhalduse lahendamine isikutele, kellele Eesti avalik sektor pakub teenust seaduse või määruse ja mitte lepingu alusel. Kuna tegu on küllalt abstraktse lahendusega[7], võib süsteemi kasutada ka muuks otstarbeks (näiteks kontaktandmete juhtimine, pääsuhaldus erasektoris vms.) kas mõningaste muutustega kasutajaliideses või üldse ilma muutusteta.

Pakutava lahenduse skoopi ei kuulu:

- igasugune identiteetide (juriidilised ja eraisikud ning igasugused muud olemid, millega on isikutel võimalik seoseid omada) väljastamine ning elutsükli juhtimine. Samuti on lahenduse skoobist väljas kasutajate tuvastamine.

[7] Objektidevaheliste suhete juhtimine on levinud ülesanne.

- mitmepoolne volitamine esindusõiguse erindite korral, kus mitu ühiselt esindusõigust omavat isikut väljendavad ühiselt tahet rolli määramiseks[8].
- vastamine päringutele rollide kehtivuse kohta minevikus. Ehk, vastus küsimusele "kas isikute X ja Y vahel eksisteerib seos A" vastatakse ainult viimase parima teadmise alusel. Süsteemile ei saa esitada päringut "kas isikute X ja Y vahel eksisteeris ajahetkel Z seos A".
- pääsuõiguste eneste juurdepääsupiirangud. Kõik pääsuõigused on klientsüsteemide ja vastavate õigustega kasutajate (isik ise ja kõik teda esindavad isikud) jaoks avalikud. Ehk, süsteem ei ole sobilik mitteavalike rollide määramiseks. Samuti ei tohi pakutavas lahenduses kirjeldada[9] allikregistrite poolt väljastatavaid rolle, mis ei ole kõigi klientsüsteemide jaoks avalikud.

Pakutava lahenduse skoobist on väljas ka järgmised asutuste poolt püstitatud nõuded:

- **Volituse kadumine, kui volitanud isiku volitus peatub**. Näiteks, kui juhatuse liikme volitused lõpevad, lõpevad automaatselt ka tema poolt väljastatud volitused. Tegu on keerulise ning raskesti ennustatavate tagajärgedega (võivad kaduda kõik õigused) äriloogikaga, mis on läbiviidud intervjuude põhjal kasutusel ainult KeMITis. Vajadusel võivad selle loogika realiseerida klientsüsteemid
- **ACL[10] volituste alusel**, mis on kasutusel Statistikaametis. Selle loogika alusel võib ettevõtte esindaja anda erinevatele rollidele erinevad õigused aruannete esitamiseks. Funktsionaalsuse vajadus ei ole lõpuni selge[11] ning näiteks Päästeametis on vastav funktsionaalsus lahendatud täiesti ilma volituseta võimaldades igal autenditud kasutajal lisada pärast vastava valeandmete esitamise tagajärgi kirjeldava teksti läbi lugemist lisada aruandeid ükskõik kelle nimel
- **Puukujuline rollipuu**, kus igal rollil võib olla piiramatu hulk alamrolle. Näiteks võib raamatupidaja rollil olla alamroll "pearaamatupidaja", kellel on veel õigusi lisaks raamatupidaja õigustele. Kuigi tehniliselt küllal lihtsasti realiseeritav muudaks selline

[8] Vt p 3.3.3.
[9] Mis ei tähenda, et pakutavas lahenduses kirjeldatud standardeid ei tohiks kasutada osapoolte omavaheliseks suhtluseks. Allikregister võib realiseerida pakutavas lahenduses kirjeldatavatele standarditele vastava x-tee päringu rollide kohta ja teha selle kättesaadavaks vaid näiteks seaduses määratud osapoolele.
[10] *Access Control List*, eesti keeles pääsuloend.
[11] Aruande esitamise õigus ei pea tähendama ka aruannete nägemise õigust, nii ei saa lihtsalt andmeid esitades tekkida ligipääsu konfidentsiaalsele infole.

rollide seoste loogika rollide nimekirja navigeerimise keerulisemaks ning raskendaks mõistliku kasutajaloogika pakkumist. Seejuures on vajadus rolle mõistlikult grupeerida selgesti olemas ning seda funktsiooni täidavad pakutud lahenduses nimeruumid

- **Paberil, käsitsi, telefonitsi, üles laetud dokumendi kaudu vms. volituste vastu võtmine**. Ehk, keskne pääsuhaldussüsteem pakub ainult iseteeninduslikku pääsuõiguste haldust[12]. Kui asutusel on vastava äriprotsessi vajadus, võib ta selle realiseerida oma infosüsteemide raames ning tulemuse standardsete liideste kaudu kesksele süsteemile kättesaadavaks teha
- **Rolli volitatud isikute hulga piiramine**. Ehk, igasse rolli võib kuuluda ainult piiratud hulk isikuid. Vajadus on teadaolevalt piiratud Statistikaametiga. Tarbe korral saab vastava funktsionaalsuse lahendada asutuse enda poolel. Äriloogilises mõttes on tegu piiratud kasulikkusega funktsiooniga mis ühtlasi lisab olulisel määral tehnilist ja funktsionaalset keerukust luues vajaduse näiteks lahendada olukordi, kus ainus kasutaja loobub rollist või samaaegselt üritavad eri inimesi hulgaga piiratud rolli lisada eri volitatud isikud

3.2. Nõuded

Kuna süsteemile esitatud funktsionaalne vajadus on olemuslikult lihtne (isiku võimalus määrata teisele isikule mõnda rolli), on ka püstitatud nõuded enamasti väljendatavad konkreetset funktsionaalsust realiseerivate kasutuslugude ja isegi mitte äriprotsessi kaudu.

Siiski on tuvastatud funktsionaalsed nõuded, mida pakutav süsteem kindlasti täitma peab:

- võimalus määrata rollile aegumistähtaega; ja
- võimalus nõuda, et rolli määramisel kinnitab volitaja oma tahet elektroonilise allkirjaga.

[12] Analüüsi käigus esile kerkinud vajadust kontrollida notariaalsete volituste kehtivust tuleb lahendada väljaspool käesoleva süsteemi realisatsiooni skoopi. Näiteks võib luua eraldi notariaalsete volituste registri ning selle kesksele pääsuhaldusele allikregistrina kättesaadavaks.

3.3. Üldist

3.3.1. Seosed

Pakutav lahendus tugineb mõnevõrra abstraktsele seoste kontseptsioonile. Süsteemi konfiguratsioon kirjeldab võimalikke seoseid objektide vahel ning allikregistrid või keskne pääsuhalduslahendus hoiavad konkreetseid seoseid.

Objektide A ja B vahel öeldakse olevat seos X, kui mõne nimeruumi definitsiooni järgi leidub valiidne kolmik A:X:B. Seosed ei ole transitiivsed[13]: seosest A:laps:B ei tulene, et B:laps:A ning loogikat "leidub seos A:laps:B järelikult peab leiduma ka seos B:lapsevanem:A" ei toetata[14]. Põhjuseks ei ole siin mitte tehnilised raskused vaid vajadus hoida lahendus lõppkasutajale arusaadav ning loogiliselt terviklik: kui roll "laps" võib olla defineeritud bioloogiliselt, siis roll "lapsevanem" võib olla defineeritud näiteks hooldusõiguse kaudu. Iga seose puhul on määratletud nii A kui B identifikaatori tüüp.

Seosed on jagatud nimeruumidesse. Igal nimeruumil on konkreetne omanik asutuse näol, nimeruumi konfiguratsiooni uuendamine toimub kasutades vastavat masin-masin liidest. Nimeruumidest saab viidata teiste nimeruumi rollidele.

Igas nimeruumis on määratud vaikimisi rollide lisamiseks ja eemaldamiseks vajalikud rollid, iga rolli juures saab määrata eraldi lisamiseks ja eemaldamiseks vajalikke rolle.

Iga kirjeldatud seose puhul on määratud ka A ja B identiteetide tüübid. Näiteks seos "laps" võib eksisteerida ainult eraisikute vahel. Seejuures võib pakutud lahenduses kasutajaliideses kontrollitavate seoste puhul B tüübiks olla ainult kas eraisik või juriidiline isik - kasutajaliideses toetatakse ainult nende objektide otsingut[15].

Seose tüüpide puhul on oluline rääkida hulkadest. Näiteks kõikide asutusega A seoses "juhatuse liige" olevate isikute hulk või kõikide isikuga A seoses "eestkostja" olevate isikute hulk. Hulkade puhul saab omakorda rääkida hulgatehetest, ühendist ja ühisosast. Hulkade ühendi puhul kuuluvad uude hulka kõik mõlema hulga elemendid (isikud, kellel on

[13] Teisisõnu, seosed ei ole pööratavad.
[14] Mis ei tähenda, et nimeruumi haldaja ei võiks vastavaid rolle määratleda ning alusregister vastavaid seoseid väljastada. Kindlasti on võimalik määrata seosed "juhatuse liige" ja "juhatuse liikmena esindatav", millest esimene on seos juriidilise ja eraisiku ning teine seos eraisiku ning juriidilise isiku vahel.
[15] Tegu on süsteemi funktsionaalse skoobi ja mitte tehnilise piiranguga. Vajadusel võib luua milliste iganes objektide otsingulahendusi

asutusega A seos "juhatuse liige" või seos "täievoliline esindaja") ning ühisosa puhul ainult need, mis kuuluvad mõlemasse hulka (isikud, kellel on isikuga A seos "lapsevanem" ja kellel on isikuga A seos "eestkostja"). Kui kontrollitakse seost A:X:B, siis kontrollitakse sisuliselt olemi B kuulumist teatavasse hulka. Nii on võimalik seoseid määratleda hulgateoreetiliste tehete kaudu.

Nimeruumi konfiguratsiooni puhul on seos kirjeldatud kui kas ühend või ühisosa järgmistest hulkadest, milledest kumbki võib olla tühi:

- Isikud, kellele on keskses pääsuhaldussüsteemis vastav roll määratud; ja
- Isikud, kelle osas mõni allikregister vastab jaatavalt seose olemasolu kohta.

Nii on võimalik kirjeldada nii rolle, mis on keskselt määratavad, rolle mille kohta tuleb informatsioon allikregistrist kui ka rolle, mille puhul on võimalikud mõlemad variandid. Näiteks saab nii lahendada üleminekuperioodi infosüsteemide integratsiooni puhul, kus vanad õigused tulevad veel infosüsteemist endast kuid uued määratakse juba keskses lahenduses.

Lisaks kirjeldatutele on võimalik lisada ka kolmas valik ("arvutatavad rollid"), mis koosneb hulgateroreetilistest tehetest[16]. Nii oleks võimalik määratleda kuitahes keerulisi rollide kombinatsioone: rollis "toimiku vaataja" on isikud, kellel on toimikuga seoses "hageja" oleva organisatsiooniga seoses "juriidiline esindaja" oleva organisatsiooniga seos "advokaat" või "advokaadi abi" ja kes samal ei ole seoses "toimiku vaataja" organisatsiooni suhtes, kellel on toimikuga seos "kostja"[17].

Iga keskses pääsuhalduses määratava rolli kohta on pakutavas lahenduses kirjas näiteks tema inimloetav nimi, abiteksti viide, määramiseks vajalikud rollid[18] ja eemaldamiseks vajalikud rollid[19].

Iga allikregistrile viitava rollikirjelduse puhul on kirjelduses lisaks inimloetavale nimele ka näiteks allikaviide x-tee terminites.

---

[16] Kuigi Google Zanzibar seda võimaldab, ei ole praktiline vajadus nii keeruliste seosekirjelduste järele üheselt selge. Seetõttu on tegu funktsionaalsusega, mida ei saa lugeda süsteemi kui terviku toimimiseks hädavajalikuks.
[17] Arusaadavuse huvides ei ei ole tegu formaalselt korrektse seose kirjeldusega, kuna kirjeldus viitab iseendale.
[18] Edasi volitamiseks peab see rollide nimekiri sisaldama ka rolli ennast.
[19] Rollist loobumiseks peab see nimekiri sisaldama ka rolli ennast.

3.3.2. Identifikaatorid

Identifikaatorid on objekti üheselt identifitseerivad. Igal isikul, organisatsioonil, majandusüksusel vms. on täpselt üks identifikaator, erinevad identifikaatorid loetakse eri objektideks.

Identifikaatoreid kasutatakse universaalse ressursiidentifikaatorina (URI-na)[20] viisil, mis seob konkreetse identifikaatori konkreetse kirjelduse ja nimeruumiga võimaldades eristada isikukoodi äriregistrikoodist või näiteks Leedu isikukoodi Eesti isikukoodist ilma vajaduseta registripäringu järele.

Igas nimeruumis võib defineerida identifikaatori tüüpe määratledes tema inimloetava nime allika. Ehk, seose 37508166515:laps:51107050123 puhul on vajalik, et mõnes nimeruumis oleks määratletud teenus, mille kaudu on võimalik isikukoode parasjagu kehtivaks nimeks lahendada.

Isiku rollide erinevate pääsuõiguste[21] lahendamine toimub kas:

- klientsüsteemi poolel. Seejuures päritakse kõik esindatavad isikud, lubatakse kasutajal nende hulgast valida ning sellest valikust tulenevalt piiratakse äriloogiliselt kasutaja ligipääsu funktsionaalsusele; või
- arvutatavate rollide mehhanismiga. Seejuures kirjeldatakse roll, mis võtab arvesse isiku teisi rolle (nagu eelkirjeldatud juriidiliste esindajate näites).

3.3.3. Juriidiliste isikute esinduse erindid

Eestis võivad juriidiliste isikute esindusõigust omada nii iga juhatuse liige eraldi kui juhatuse liikmed kas kõik koos või erinevates kombinatsioonides. Tegu on teenusepakkuja jaoks ebamugava olukorraga. Kuigi äriregister väljastab vastavat informatsiooni ka täna masinloetaval kujul, tuleb mitme osapoolega esindusõiguse korral iga konkreetses äriprotsessis sisalduva otsuse fikseerimiseks määramiseks realiseerida keeruline, paljude osapoolte aktiivset kaasamist nõudev ja habras äriprotsess. Samasugune protsess tuleks

[20] https://et.wikipedia.org/wiki/%C3%9Chtne_ressursiidentifikaator.
[21] Isik B kui asutuse A esindaja vs. isik B, kui eraisik. Esimesel on ligipääs asutuse A andmetele ja teisel mitte.

realiseerida ka juhul, kui hulk juhatuse liikmeid ühiselt määrab ühe konkreetse esindaja. Kuna esindaja valik ei ole olemuslikult mitte pääsuõiguse määramise vaid esindusõiguse valiku juriidilise sisuga protsessiga, ei ole seda mõistlik realiseerida pääsuhalduse lahenduses. Samal põhjusel ei ole mõistlik keskselt lahendada näiteks eestkostja määramise protsessi.

Küll aga saab pääsuhalduse lahendus esindusõiguse informatsiooni vahendada, kui luuakse eraldi äriprotsess, mille kaudu on juhatuse liikmetel võimalik määrata ühise esindamise juhtudel enda seast esindaja. Üheks võimaluseks on määratleda kaks eraldi rolli: "täievoliline esindaja" (ühise esindamise juhul teiste juhatuse liikmete poolt valitud esindaja) ja "juhatuse liige". Eraisik võib kuuluda nii mõlemasse rolli korraga kui ka vaid ühte neist. Sellise lahenduse korral on osapooltel mitu võimalust toimimiseks.

Näiteks, kui äriregister väljastab kõigi juhatuse liikmete kohta, kes ka üksinda võivad juriidilist isikut esindada, kuulumise mõlemasse rolli, saavad teenusepakkujad valida, kumb neist (nn täievoliline esindaja või juhatuse liige) vastab täpsemini nende vajadusele. Teenusepakkujad, kelle nõuded esindusele ei ole kõrged, uurivad kasutaja kuulumist kas juhatuse liikme või täievolilise esindaja rolli. Teenusepakkujad, kelle jaoks on oluline juriidiliselt tähenduslik esindusõigus, kontrollivad vaid täievolilise esindaja rolli olemasolu. Kui teenusepakkuja vajalikuks peab, võib ta kasutajad, kes on juhatuse liikmed kuid mitte täievolilised esindajad, suunata nende jaoks loodud ja äriregistri andmetele tuginevasse esindaja valimise äriprotsessi.

Äriregister (või muu osapool, nt MTA)[22] võib ka otsustada, et võimaldab juriidilistel isikutel valida endi seast täievolilise esindaja toiminguteks elektroonilises kanalis ning realiseerida vastava äriprotsessi. Sel juhul väljastab ta lisaks täievolilise esindusõigusega juhatuse liikmetele vastava rolli ka uue äriprotsessi kaudu valitud isikute kohta. On oluline tähele panna, et sel juhul ei muutu klientsüsteemide jaoks midagi: nad saavad jätkuvalt pärida juhatuse liikme ning täievolilise esindaja rollide kohta, saada juriidiliselt pädeva vastuse ning kasutada kumbagi rolli või nende kombinatsioone vastavalt oma äriprotsessi

[22] Kui rolli „täievolilise esindaja" allikregistriks ei ole ÄR, vaid nt MTA, siis muudetakse konfiguratsiooni nii, et rolli "täievoliline esindaja" allikregistriks ei ole enam mitte äriregister vaid valikuprotsessi realiseerinud osapool, näiteks MTA.

vajadustele. Lõppkasutaja jaoks ei muutu samuti midagi peale võimaluse saada esindaja valiku äriprotsessi läbi juurepääsu seni ligipääsut teenusele.

See, kas ja kuidas selline „täievolilisise esindaja“ valimise ja pärimise protsess realiseeritakse, on väljaspool antud analüüsi ning tegemist on võimaliku lahendusega juriidiliste isikute esinduse erindite probleemile.

3.3.4. Nimekirjade tugi

Sageli sõltuvad kodaniku pääsuõigused tema kuulumisest (või mittekuulumisest) mõnda konkreetsesse nimekirja. Kuigi sellised nimekirjad võivad olla asutusesised (näiteks nimekiri konkreetset litsentsi omavatest juriidilistest isikutest), võivad need olla ka asutustevahelise iseloomuga (näiteks ärikeelud).

Sellised seosed saab pakutavas lahenduses realiseerida seostena isiku ja allikiregistri vahel. Näiteks võib ärikeeld olla realiseeritud seosena nimega "ärikeeluga_isik" isiku ja äriregistri vahel. Nii on võimalik esitada kas äriregistrile või kesksele pääsuhalduse lahendusele küsimus "kas isikul B eksisteerib roll ärikeeluga_isik äriregistri suhtes". Seejuures pöördutakse vastuse saamiseks äriregistri poole täpselt sama liidese kaudu, mille kaudu saab vastuse küsimusele "kas isikul B eksisteerib juhatuse liikme roll asutuse A suhtes".

Selliseid rolle, nagu ka kõiki teisi allikregistrile tuginevaid rolle, ei saa kasutajaliideses muuta, kuid need on selle kaudu vaadeldavad.

Nii lähenedes on eri asutustel võimalik oma kontrollitavates nimeruumides määratleda millise iganes sisuga nimekirju, mida nad avaldada soovivad. Samas tekib aga vastutus ka nimekirju standardsel viisil kättesaadavaks teha.

Vajadusel võib sedalaadi nimekirjade abil lahendada ka suurema osa aktiivses kasutuses olevatest atribuudipõhise pääsuhalduse vajadustest koostades näiteks nimekirja elus inimestest (seos "elus" isiku ja rahvastikuregistri vahel) või täisealistest inimestest (seos "täisealine" isiku ja rahvastikuregistri vahel).

3.3.5. Funktsionaalsus

Osana kesksest pääsuhalduse lahendusest realiseerib pakutud lahendus vähemalt järgmise funktsionaalsuse:

1. Kasutaja saab volitada isikut A rolliks B. Nii A kui B võivad olla kas eraisikud või ettevõtted ning kasutajal peab olema volituse andmiseks vajalik õigus isiku A suhtes
2. Kasutaja vaadata kõiki volitusi ja isikuid, mis on seotud (antud kas neile või nende suhtes) kas tema endaga või mõne isikuga, kelle suhtes tal on vastavad õigused
3. Kasutaja saab volitusi eemaldada
4. Nimeruumi haldaja saab masinliidese abil üles laadida uue nimeruumi konfiguratsiooni
5. Väline süsteem saab lisada, eemalda või kontrollida volitust masinliidese abil

Lisaks primaarsele funktsionaalsusele võib pakutav lahendus realiseerida ka järgmise funktsionaalsuse:

1. Süsteem suudab konfiguratsiooni alusel hulgatehete abil vastata küsimustele seoste kohta, mis on defineeritud teiste seoste kaudu (näiteks: "inimesed, kellel on seos A ja ei ole seost B või inimesed kellel on seos C")
2. Süsteem suudab kasutajat teavitada erinevatest sündmustest (volituse lisamine, eemaldamine, aegumine aga ka näiteks töölepingu lõppemine rolliga seotud juriidilise ja füüsilise isiku vahel[23]) kas talle, temaga seoses või tema poolt määratud rollidega
3. Süsteem suudab kasutajale anda soovitusi rollide osas, mida võiks isikule veel lisada vähendamaks vaeva, mis kulub levinumate rollide otsimisele ning määramisele
4. Ettevõtte esindaja või eraisik võib saabuda keskkonda läbi veebipõhise OAuth[24] voo, lisada sisendandmete põhjal volituse ja selle (vajadusel) allkirjastada

[23] Seoste automaatseks lõpetamiseks on mõislikum kasutada seoste kirjeldust määratledes seose ühisosana neist, kellel on määratud vastav roll ja neist, kellel eksisteerib esindatavaga töösuhe.
[24] Standardne protokoll volituste palumiseks ja andmiseks veebikeskkonas. Sellise kasutusloo realiseerimisel saab teenusepakkuja, näiteks Xolo, suunata kasutaja kesksesse pääsuhalduse keskkonda neile vajalikke volitusi andma.

4. Tehniline lahendus

4.1. Keskne süsteem

Pakutava lahenduse keskset süsteemi võib realiseerida mitmel eri moel ning, kuni eelkirjeldatud käideldavusnõuded on täidetud, ei ole realisatsiooniks valitud tehnoloogia funktsionaalsuse saavutamisel kriitiline. Siiski on rida olulisi väljakutseid, mille puhul tõenäoliselt ei ole samaväärseid alternatiive järgnevatele lahendusi:

- Kõikidest allikregistrist päritavatest seostest hoitakse kohalikku koopiat[25]. Nii tagatakse pääsuhalduslahenduse käideldavust ning kaitstakse allikregistreid liigse ja potentsiaalselt ebaühtlase koormuse eest. Talletatakse ainult identifikaatorite ja seose andmeid, muid atribuute ei käidelda. Väliste allikate uuendamine käib kolmel viisil:
    - Kasutades standardset lisa/eemalda seos liidest, mida kutsub välja kas allikregister või allikregistri sõnumeid tõlkiv adapter.
    - Kasutades standardset nimekirjapõhist adapterit, mis perioodiliselt käivitudes loeb konfiguratsioonist infot vastava liidest realiseerivate allikregistrite kohta ning esitab vastaspoolele päringu "anna kõik seosed A:B:X", kus X on konfiguratsioonist leitud rolli nimi
    - Kasutades spetsiaaladapterit, mis realiseerib oma päringu- ja koopialoogika
- Kasutaja poolt määratavaid ja allikregistritest päritavad seoseid hoitakse nende erinevate koormusprofiilide ja mahtude tõttu kirjutamise tarbeks eraldi andmebaasides. Samas lugemiseks mõeldud andmebaasi instantsides võivad mõlemat liiki seosed olla kombineeritud
- Identifikaatoriga seotud inimloetav nimi tuuakse päritakse asünkroonselt kasutajaliidese kaudu kasutades siiski autenditud sessiooni. Ehk, päring "mis nimi vastab isikukoodile 37508166515" tuleb koos sessioonivõtmega otse kasutaja brauserist ning suunatakse pärast sessioonivõtme valideerimist kas konfiguratsioonist leitud x-tee teenusele või lahendatakse kohaliku puhvri abil. Nii välditakse liigset andmete kogumist kesksesse pääsuhalduslahendusse, tagatakse

[25] Eeldusel, et andmete töötlemiseks õnnestub leida andmekaitse regulatsiooniga sobiv tehniline ja juriidiline lahendus.

alati värskeima võimaliku nime kuvamine kasutajale ning lahutatakse ärikriitilised päringud sekundaarsetest

- Soovituste andmise puhul[26] arvutatakse need kui mitte ärikriitilised perioodiliselt ja mitte reaalajas. Ühena võimalikest võib kasutada järgmist algoritmi:
    - Loo nimekiri rollidest sorteerituna nende esinemissageduse järgi
    - Moodusta nimekirja alusel puu paigutades juureks tühi hulk ning lisades iga n-taseme tipule kaks alamtippu, milledest ühes on hulk, mis sisaldab rollide nimekirjas n+1 kohal asuvat rolli ja teises hulk, mis seda ei sisalda. Tulemuseks on puu kõigist võimalikest rollide hulga alamhulkadest
    - Iga mittetühja alamhulga A kohta puus :
        - käivita päring, mis leiab kõik rollid ja nende arvu, mis on identiteetidel, kellel on kõik alamhulka kuuluvad rollid
        - Lahuta tulemusest alamhulk A
        - Sorteeri tulemus esinemissageduse järgi
        - Salvesta A juurde kõige sagedasemat 5 rolli koos nende esinemissageduse ja protsendiga (suhtes algses päringus esinenud identiteetide arvuga)

4.2. Allikregistrid

Allikregistrid moodustavad kriitilise osa pakutavast lahendusest. Allikregistri pidaja peab pakutavas lahenduses realiseerima liidesed, mis võimaldavad nii kesksel pääsuhalduslahendusel kui teistel süsteemi osalistel registrisse standarditele vastavaid päringuid esitada.

Kuna allikregistri määratlus tuleneb nimeruumi konfiguratsioonist, on eeldatav tihe koostöö[27] konfiguratsiooni haldava ning nimeruumi peamisi allikregistreid käitava organisatsiooni vahel. Tõenäoliselt on mõistlik need rollid ühitada.

Lisaks ilmselgetele allikregistritele nagu äriregister ja rahvastikuregister on tõenäoliselt vaja määratleda ka teisi allikregistreid. Näiteks Statistikaamet opereerib majandusüksuse

[26] Vt p 3.3.5.
[27] Vt p 2.2.

mõistega, võimaldab nende suhtes rolle määratleda ning seega peab keskse pääsuhalduse mõistes toimima kui allikregister.

Lisaks juriidilise tähendusega registripäringutele võib allikregistrina toimida ka kuitahes keerulist äriloogikat realiseeriv komponent. Näiteks võib leiduda komponent, mis vastab küsimusele "kas kodanikul X on õigus osta kodaniku Y ravimid", mis kasutab nii rahvastikuregistri, sotsiaalkaitse andmekogu, kohtulahendite kui mis iganes muu andmekogu andmeid. Sealaadi komponent võib olla üldine ("Kodanikul X on õigus esindada kodanikku Y") kui ka spetsiifiline (ravimite ostu näide). Seejuures ei ole tegu avaliku teabe seaduse rikkumisega kohutuse mõttes küsida andmed otse allikast, sest nii defineeritud allikregister ei vasta mitte küsimusele "kas kodanikul X on kodaniku Y suhtes roll Z" vaid konkreetsemale küsimusele näiteks vanemliku suhte, hooldusõiguse, hooldekodus viibimise vms kohta.

4.3. Klientsüsteemid

4.3.1. Üldist

Klientsüsteemi integratsiooniks keskse pääsuhalduse ökosüsteemi on pakutavas lahenduses mitmeid võimalusi. Integratsioonimudelite paljusus on süsteemi üheks oluliseks edufaktoriks, sest suure hulga eri infosüsteemide kaasamiseta ei saa kasutajale pakkuda keskset ülevaadet tema poolt antud või saadud volitustest kogu riigi infosüsteemis. Suurt hulka eri infosüsteeme ei saa aga kaasata võimaldamata kõigil neil leida just konkreetsesse situatsiooni sobivaim integratisoonilahendus.

Järgnevas kirjeldatakse nelja peamist integratsioonimudelit, mida võib omavahel ajas ja ruumis kombineerida: konkreetne infosüsteem võib pääsuhalduse süsteemi suhtes täita ajas muutuvaid rolle ning näiteks võimaldada teatud rollide juhtimist keskselt kuid teiste puhul nõuda kasutaja siirdumist teenusepakkuja keskkonda.

Integratsioonimudeli valik sõltub ka klientsüsteemile püstitatud käideldavusnõuetest. Kõrgete käideldavusnõuetega süsteemide puhul on mistahes välise sõltuvuse lisamine ebasoovitav ning seega on soovitatav kas minimaalne või osaline integratsioon.

4.3.2. Täisintegratsioon

Selle mudeli puhul loobub teenusepakkuja täielikult pääsuhalduse info kogumisest, hoidmisest ja töötlemisest. Kõik kasutatavad rollid on kirjeldatud mõnes nimeruumis ning klientsüsteem pärib kasutaja vajalikud rollid otse kesksest pääsuhalduse lahendusest. Kõik kasutatavad rollid on seatavad ja eemaldatavad ainult keskse pääsuhalduslahenduse kaudu.

4.3.3. Minimaalne integratsioon

Minimaalse integratsioonimudeli korral säilitab klientsüsteem kogu oma pääsuhalduse lahenduse ning kesksele kasutajaliidesele tehakse standardsete liideste kaudu kättesaadavaks rollide lugemise ja eemaldamise liidesed. Kesksesse kasutajaliidesesse sisse loginud kasutaja näeb süsteemis antud volitusi ja saab neid vastavate õiguste olemasolul eemaldada, kuid õiguste lisamiseks suunatakse ta klientsüsteemi. Klientsüsteem võib realiseerida kuitahes keerulise rollide jagamise, edasijagamise või tuletamise süsteemi ning võimaldada kasutajal kombineerida rolli-, nimekirja- ning atribuudipõhist pääsuhaldust. Ainsaks piiranguks on nõue kirjeldatud seosed standardsel viisil kättesaadavaks teha.

Kõik kesksele pääsuhalduse lahendusele kättesaadavaks tehtud rollid on kirjeldatud mõnes nimeruumis.

4.3.4. Osaline integratsioon

Osalise integratsiooni puhul säilitab klientsüsteem oma pääsuhalduse lahenduse ning kesksele süsteemile tehakse kättesaadavaks rollide lugemise, eemaldamise ning lisamise liidesed. Kõik rollid on kirjeldatud mõnes nimeruumis ning klientsüsteem võib kasutada pääsuhalduseks ka teisi keskselt hallatavaid rolle.

4.3.5. Alliksüsteemi integratsioon

Selle, kõige lihtsama, integratsioonimudeli korral ei kasuta klientsüsteem ei keskset pääsuhalduslahendust ega realiseeri ka enda oma. Selle asemel kasutatakse mõne

alliksüsteemi poolt pakutavat standardset liidest näiteks juriidilise isiku esindusõiguse kindlaks tegemiseks. Nii on vajaduste muutudes võimalik integratsioonipunkti muutmata sujuvalt liikuda mõnele teise integratsioonimudelile.