PROUD ENGINEERS

Keskne volituste, rollide ja pääsuõiguste haldamise süsteem

Tulevikulahenduse arhitektuur

Koostaja: Proud Engineers OÜ

Versioon: 2.0

Kuupäev: 14.12.2021

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

Sisukord

Mõisted ja lühendid

Mõiste või lühend	Selgitus
Allikregister	**Allikregister** on infosüsteem, kes haldab nii andmete töötlemise kui ka andmeid tekitavate äriprotsesside mõttes mõnda seost isikute vahel[1]. Näiteks haldab äriregister infot juriidiliste isikute esindusõiguste kohta ning käitab ka äriprotsesse, mille käigus isik võib juriidilise isiku esindusõiguse omandada või selle kaotada. Seega on äriregister kirjeldatavas lahenduses esindusõiguste allikregister. Sama roll on rahvastikuregistril näiteks laps-vanem seoste osas.
E-ITS	Eesti infoturbestandard (**E-ITS**) pakub organisatsioonile infoturbe riskidega toimetulekuks infoturbe halduse süsteemi, aidates seeläbi keerulisel infoturbemaastikul teha kvaliteetseid juhtimisotsuseid.
Identiteedipakkuja	**Identiteedipakkuja** on infosüsteem, kes suudab keskse pääsuhalduse lahenduse poolt kasutatavaid identifikaatoreid lahendada inimloetavateks nimedeks. Tüüpiliselt on identiteedipakkuja ka allikregister.
Klientsüsteem	**Klientsüsteem** on infosüsteem, kes toimib keskse pääsuhalduse lahenduse suhtes kliendina kas pärides infot oma kasutajate rollide kohta või tehes selle info kesksele lahendusele lugemiseks ja/või muutmiseks kättesaadavaks.
KOV	Kohalik omavalitsus (**KOV**)
Nimeruum	**Nimeruum** on kogum rollide kirjeldusi, mida haldab üks pääsuhalduse lahenduse osapooli. Kõik rollid kuuluvad nimeruumidesse. Nimeruumide viitamisel kasutatakse notatsiooni a#b, mida tuleb lugeda "roll b nimeruumist a".
OAuth	**OAuth** (täpsemalt OAuth 2.0) on standardne protokollistik, mille abil süsteem saab paluda kasutajal autoriseerida ligipääs kaitstud ressursile ning kaitstud ressursi valdaja saab kontrollida vastava autoriseeringu olemasolu. Standardit kirjeldavad RFC 6749, RFC 6750, RFC 6819 ja teised.
PaaS	***Platform as a Service*** on süsteemide haldamise mudel, kus komponentide käitamiseks vajalikku taristut kuni operatsioonisüsteemini pakutakse kasutades jagatud taristut
RFC	*Request For Comments* (**RFC**) on standardiseeritud viis (enamasti internetiga seotud) standardite kokku leppimiseks ja dokumenteerimiseks.
RIA	**Riigi Infosüsteemi Amet**
Roll	**Roll** või **volitus** on seos kahe isiku vahel. Näiteks kui eraisik on juriidilise isiku juhatuse liige, öeldakse eraisiku ja juriidilise isiku vahel olevat seos "juhatuse liige", või teisiti öeldes, eraisikul on juriidilise isiku suhtes roll "juhatuse liige". Rollidest rääkimisel kasutatakse notatsiooni A:B:X, mida tuleb lugeda "B on A suhtes rollis X". Esimest nii mainitud notatsioonis toodud isikut kutsutakse A-osapooleks (isik, kelle suhtes roll eksisteerib), teist B-osapooleks

[1] Tehniliselt võttes on keskne pääsuhalduse lahendus samuti allikregister, kuna haldab nii protsesse teatud õiguste määramiseks kui ka infot õiguste kohta. Nii on keskne pääsuhalduse lahendus ka mõeldud käituma pärides pärast kasutaja autentimist iseenda käest infot kasutaja esindatavate isikute kohta.

	(isik, kes on rollis)[2]. Kõik mõne isikuga mõnes rollis olevaid isikuid tähistavatest hulkadest rääkides kasutatakse järgmist notatsiooni: • ***:B:X** - Kõik sellised isikud, kellega B on seoses X; • **A:*:X** - Kõik sellised isikud, kes on A-ga seoses X; • **a.b** - Kõik sellised isikud, kes on seoses b isikuga a; • **a.b.c** - Kõik sellised isikud, kes on seoses c mõne isikuga, kes on seoses b isikuga a.
RTK	Riigi Tugiteenuste Keskus (**RTK**) pakub riigiasutele administratiivseid teenuseid, sealhulgas finants- ja personaliarvestust
Seos	Vt Roll.
TARA	**Riigi autentimisteenus** on RIA poolt käitatav keskne autentimisteenus
Tooken	Tooken (ingl. *token*), tuntud ka kui volitustõend on objekt, mis tõendab õigust sooritada mingit toimingut
Volitus	Vt Roll.

[2] A ja B osapooled ei ole omavahel vahetatavad. Vaata lähemalt punktist 4.

Muudatuste ajalugu

Versioon	Kuupäev	Kommentaar
1.1	18.10.2021	• Lisatud märkused andmesubjektide õiguste kaitse kohta otsingus kasutuslugudesse ja rajadokumenti • Lisatud märkus pilvetaristu kasutamise organisatoorsete tagajärgede kohta • Täiendatud lühendeid ja mõisteid • UC38 juurde toodud lisaks TARA-le ka eesti.ee näide • Lisatud viited RIA ja riigi taseme mittefunktsionaalsetele nõuetele • Lisatud sõltuvuste halduse alajaotus (6.2.13) ja uuendatud sisukord
1.2	04.11.2021	• Lisatud märkus rollide konfiguratsiooni dokumenteerimisvajaduse kohta
1.3	07.11.2021	• Parandatud pisivead tekstis • Läbi viidud keelekontroll
1.4	15.11.2021	• Sissejuhatusse lisatud viite algallikate kohta
1.5	02.11.2021	• Lisatud märkus sõnumiliidese üldise olemuse kohta • Täiendatud märkust digiallkirja süsteemi olemasolevate lahenduste kohta • Lisatud märkus eesi.ee kohta sissejuhatusse • Kontaktandmete haldus muudetud väliseks funktsiooniks: kasutajahaldur märgitud liidest tarbivaks komponendiks, lisatud välise tarbitava liidese kirjeldus, hoidlate punktis kasutajahalduri kirjeldus muutunud, UC41 nimi ja kirjeldus muutunud • Lisatud kokkuvõte
2.0	09.12.2021	• Kasutuslugude kirjeldused tõstetud eraldi dokumenti. Uuendatud kõik viited ja funktsiooni peatüki tekst • Tabel 1 lisatud sõltuvuste halduse protsessi veerg • Uuendatud kasutuslugude diagramme vastamaks kasutuslugude muutustele ja prototüübile • Uuendatud Lisa 1 vastavalt kasutuslugude muutustele • UC16 (Kasutaja eemaldab kõik teda esindava isiku volitused) liikunud sekundaarseks kasutuslooks • Lisatud UC50 "Kasutaja otsib volituste nimekirjast või filtreerib volituste nimekirja"

1. Sissejuhatus

Käesolev dokument kirjeldab keskse volituste, rollide ja pääsuõiguste haldamise süsteemi tulevikulahenduse arhitektuuri. Keskse volituste, rollide ja pääsuõiguste haldamise süsteemi eesmärk on võimaldada kasutajatele nii kontroll kui ka ülevaade neile või nende poolt antud õigustest ja rollide osas. Seejuures on ülesande keskmes just ettevõtjad, kes tegutsevad tihti juriidilise isiku esindajana ning kelle esindatavaid isikuid esindab sageli mitmesugustes toimingutes suur hulk teisi eraisikuid. Seejuures keskendutakse just eri osapoolte vahel potentsiaalselt jagatavatele pääsuõigustele, lahenduse skoobist on väljas ametnike ja asutustele teenust pakkuvate isikute pääsuõiguste spetsiifilised äriprotsessid, kuna need on reeglina spetsiifilised konkreetsele asutusele ja ei ole seega lihtsasti keskselt pakutavad. Siiski on kirjeldatav lahendus võimeline koguma, haldama ja jagama milliseid iganes pääsuõigusi, kui klientsüsteemid vastavad andmed kättesaadavaks teevad ning vastavad äriprotsessid realiseerivad.

Lahendatava probleemi skoop ning süsteemi eesmärk tuleneb hanke "Pääsuhalduste analüüs" (viitenumber 235557) dokumentatsioonist. Lahendus ise tugineb Eesti avalikus sektoris kasutusel olevate pääsuhalduslahenduste analüüsile[3] ning detailiseerib tulevikulahenduse kirjelduse[4].

Dokument on suunatud järgmistele sihtrühmadele:

- **Süsteemi disainer,** kes tegeleb tulevase keskse pääsuhalduse lahenduse tehnilise disainiga või peab tegema lahenduse kui tervikuga seotud tehnilisi otsuseid;
- **Tehnik**, kes hindab tulevase lahenduse loomiseks vajaliku töö ulatust, keerukust ning mahtu;
- **Tooteomanik**, kes tegeleb tulevase lahenduse organisatoorse toe loomisega ning lahenduse skoobi juhtimisega;
- **Klientsüsteemi ja allikregistri omanik**, kes otsustab integratsioonimustri keskse pääsuhalduse lahendusega ning vastutab selle realisatsiooni eest.

Dokument käsitleb kahte erinevat süsteemi: pääsuhalduse lahendus ja selle alamsüsteemi keskne pääsuhalduse lahendus. Neist esimene sisaldab endast kõiki pääsuhaldusega seotud osiseid: allikregistrid, klientsüsteemid, identiteedipakkujaid jms. Neist teine on

[3] Dokument " Keskne volituste, rollide ja pääsuõiguste haldamise süsteem. Hetkeolukorra kaardistus ja analüüs"
[4] Dokument "Keskne volituste, rollide ja pääsuõiguste haldamise süsteem. Tulevikulahenduse kirjeldus"

pääsuhalduse lahenduse keskselt paigaldatav komponent, mis pakub osapoolte koordinatsiooni ning lõppkasutaja kasutajaliidest. Seejuures on keskne pääsuhalduse lahendus kirjeldatud terviklikuna määratledes selgelt tarbitavad ja pakutavad liidesed. See ei välista, et süsteem seotakse kasutajakogemuse mõttes suuremal või vähemal määral eesti.ee keskkonnaga kuid võimaldab selgelt eristada pääsuhaldust ja muid funktsioone pakkuvaid komponente.

Dokument on jagatud järgmisteks suuremateks osadeks:

- **Funktsioon**, mis kirjeldab kõrgel tasemel seda, mida lahendus tervikuna tegema peab. Sealhulgas kirjeldatakse mittefunktsionaalsed nõuded;
- **Kontseptsioon**, mis kirjeldab antud funktsiooni realiseerimiseks valitud kontseptuaalset lahendust[5];
- **Vorm**, kirjeldab, kuidas soovitud funktsionaalsus konkreetse kontseptsiooni raames realiseeritud peaks saama;
- **Rajadokument**, mis kirjeldab süsteemi suhet ümbritsevaga tarkvara (ehk, tehnilised liidesed), orgvara (ehk, äriprotsessid) ja infrastruktuuri (sealhulgas pilvetaristu) dimensioone pidi
- **Integratsioon**, mis kirjeldab erinvaid viise keskse lahendusega liidestumiseks ning võimalusi rea kasutus-stsenaariumide realiseerimiseks

Detailsusastmelt on arhitektuuridokument mõeldud kasutamiseks osana hankedokumentatsioonist. Sellisena on tema eesmärk võimaldada hinnata lahenduse realisatsiooniks vajalikke ressursse ning ülesande keerukust. Seejuures on hoidutud tehnilistest otsustest, mis ei oma lahenduse kui terviku toimimisele mõju kuid võivad piirata pakkujate valikuvõimalusi (näiteks otsus konkreetse andmehoidla platvormi osas) või osutuda hankeprotsessi käigus aegunuks (OAuth standardi tookeni krüptoalgoritm). Samuti tuleb luua ja osapooltega kooskõlastada lahenduse toimimiseks olulised standardid.[6] Seega eeldab käesolev dokument, et lahenduse realiseerija viib enne realisatsiooni algust läbi disainiprotsessi lisades arhitektuuridokumendile tellija ja täitja koostöös puuduvad tehnilised otsused.

Käesolev arhitektuuridokument on oma olemuselt normatiivne.[7] Ta sõnastab tervikliku otsuste komplekti milledest ühe muutus põhjustab tõenäoliselt muutusi ka teistes ja/või muudab kogu kontseptuaalse lähenemise võimatuks. Siiski tuleb kasutajakogemust ja

[5] Detailsem põhjendus just selle kontseptsiooni valikuks on toodud tulevikulahenduse kirjelduse dokumendis.
[6] Vt p 5.4.
[7] Välja arvatud juhendava ja selgitava iseloomuga p 7.

infoturvet lugeda arhitektuuridokumendi suhtes ülimuslikuks. Ehk, kui kasutaja vajadusi ei õnnestu piisavalt täita või süsteemi turvalisust tagada, tuleb arhitektuursed otsused üle vaadata.

2. Lühikokkuvõte

Pääsuhalduse lahendus kui süsteem hõlmab (ning vajab toimimiseks) keskset pääsuhalduse lahendust, allikregistreid (ehk juriidiliselt tähendusliku volituste info allikaid) ja klientsüsteeme (ehk keskse pääsuhalduse lahenduse pakutavate teenuste tarbijaid). Käesolev arhitektuuridokument räägib keskse pääsuhalduse lahenduse arhitektuurist ning suhetest välismaailmaga, sealhulgas allikregistrite ja klientsüsteemidega.

Keskse pääsuhalduse lahenduse funktsionaalsus jaguneb kaheks: primaarsed kasutuslood, milleta ei ole võimalik süsteemi funktsiooni täita ning sekundaarsed, mis realiseerivad toetavaid või kasutajate konkreetseid vajadusi rahuldavaid nõudeid. Arhitektuuridokumendis kirjeldatud lahendus tegeleb nii primaarse kui sekundaarse funktsionaalsusega. Võimaldamaks hinnata funktsionaalsete muutuste mõju komponentidele on eraldi välja toodud[8] seosed komponentide ja kasutuslugude vahel.

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.

[8] Vt Lisa - Kasutuslugude ja komponentide seosed.

Keskne pääsuhalduse lahendus vajab tugevat organisatoorset taristut ka toetamaks suur hulk 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.

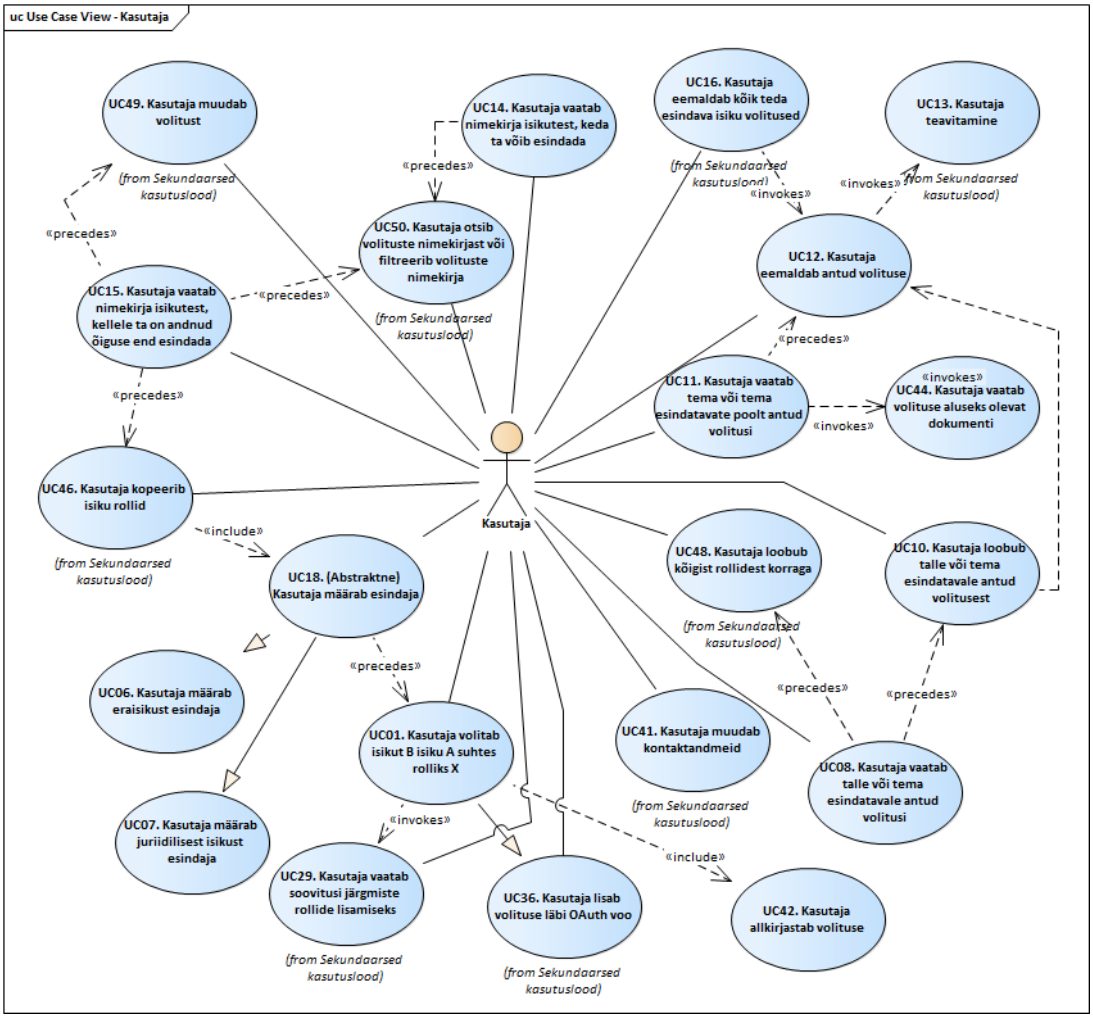
Keskne pääsuhalduse lahendus on tehnilise taristu mõttes mõeldud toimima pilvetaristul, infoturbe kaalutlustel tõenäoliselt pigem privaatsel kui avalikul. Vajalikud andmehoidlad ja ka süsteem ise on pigem kõrge lugemis- kui kirjutamisintensiivsusega ning tänapäeva mastaapides andmemahult pigem keskmise 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 nende liidestatud keskse pääsuhalduse lahenduse käideldavusele.

3. Funktsioon

Lahenduse funktsioon on pääsuhalduse info kogumine ja jagamine standarditud integratsiooni abil riigi infosüsteemiga. Seejuures lahendatakse ainult elektroonilise, internetipõhise, teenuskanali problemaatikat, füüsilise teenuskanali äriprotsesse ei käsitleta. See ei tähenda, et lahenduse abil ei saaks osapooled realiseerida füüsilise teenuskanali äriprotsesse, konkreetse äriprotsessi realisatsioon on füüsilises kanalis teenusepakkuja-spetsiifiline ning peab seetõttu olema ka tema poolt realiseeritud.[9]

Lahenduse skoop on ülesande püstituses piiratud kodanike ja juriidiliste isikutega, kes ei toimi suhtes riigiga mõne lepingu raames. Ehk, ametnike ja teenusepakkujate pääsuhaldust lahenduses ei käsitleta. Nagu ka füüsiliste kanalite äriprotsesside puhul on lahenduse paindlikkuse tõttu tema abil kahtlemata võimalik ka ametnike pääsuhalduse lahendamine (näiteks juhtudel, kus ametnikul peab olema ligipääs mõne teise asutuse teenustele), kuid sedalaadi kasutusjuhtumid ei ole lahenduse arhitektuuri loomisel ega funktsiooni kirjeldamisel olnud esikohal. Lahenduse skoobi piirangute tõttu on ka eeldatud, et B-osapooleks saab olla ainult kas juriidiline või füüsiline isik - kuigi vastava allikregistri olemasolul võib isikul olla rolle näiteks mõne katastriüksuse, auto või muu objekti suhtes, saab otsida ja rolli teiseks osapooleks lisada ainult füüsilisi ja juriidilisi isikuid.

[9] Vt p 7.2.



Joonis 1. Keskse pääsuhalduse lahenduse lõppkasutaja kasutuslood

Peamine lahenduse arhitektuuri loomise faasis tehtud funktsionaalne otsus puudutab lahenduse käsitletavat ajahorisonti: töödeldakse vaid hetkel parimat teadmist isikute pääsuõiguste kohta ja mitte teadmist isikute minevikus kehtinud pääsuõiguste kohta. Otsus tehti lähtudes sedalaadi funktsionaalsuse harvast vajadusest kuid suurest keerukusest arhitektuuri, disaini, realisatsiooni ja ka operatsioonide vaates. Seejuures on siiski võimalik määrata rollide algus- ja lõpukuupäevi tulevikus, nende alusel arvutatakse hetke parim teadmine.

Teine oluline lahenduse funktsiooni ja tehnilise struktuuri kirjeldamisel tehtud eeldus on pääsuõiguste vaba kontrollitavus: kõigil lahendusele ligipääsu omavatel klientsüsteemidel on võimalik esitada päringuid ja saada vastuseid kõigi isikute õiguste kohta kõigi teiste isikute osas. Tekkiv isikuandmete volitamata töötlemise risk on maandatav juriidiliste (kõik osapooled sõlmivad lahenduse pakkujaga vastava lepingu) ja organisatoorsete

(Andmejälgija kasutamine) meetmetega ning jääkriski suurus ei kaalu üles lisanduvat tehnilist ja kasutajaliidese keerukust.

Keskse pääsuhalduse lahendus tugineb järgmistel funktsionaalsetel nõuetel, mis omakorda on kogutud kas intervjuudest või on esile kerkinud funktsionaalsete otsustena arhitektuuri loomise protsessi käigus:

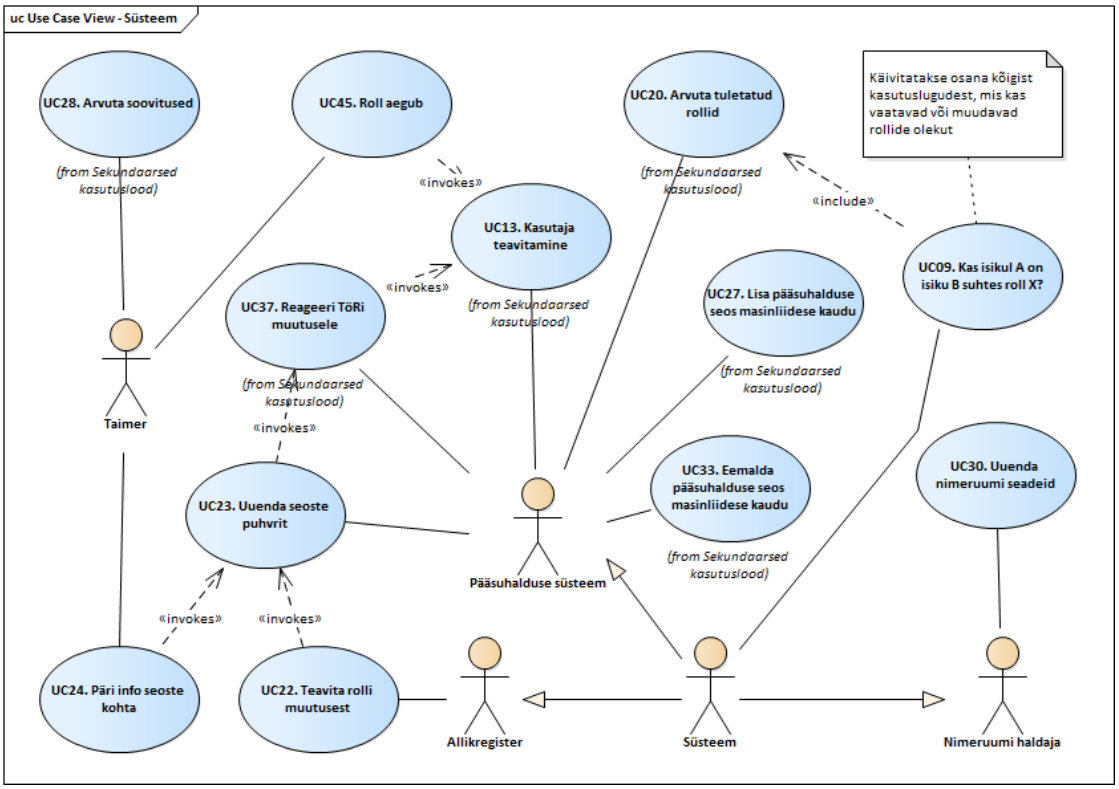
1) Kõik vastused rollide kehtivuse kohta tehakse hetkeseisuga. Seejuures on "hetke" mõiste määratletud avaldatud teenustaseme lepingus[10];
2) Peab olema võimalus määrata rolli algus- ja lõpptähtaega;
3) Peab olema võimalus nõuda, et rolli määramisel kinnitab volitaja oma tahet elektroonilise allkirjaga. Sel viisil tekkinud allkirjastatud dokument peab olema kättesaadav kogu rolli eksisteerimise aja jooksul;
4) Nimeruumide konfiguratsioon peab olema versioneeritud, kogu versioonide ajalugu peab terviklikult säilima;
5) Nimeruumide konfiguratsiooni uuendamise ja nende kehtima hakkamise aja vahel peab olema piisav (teenuslepingus sätestatud) aeg.

Keskse pääsuhalduse lahenduse kasutuslugusid kirjeldab dokument „Kasutuslugude ja prototüübi kirjeldus“. Kasutuslood toetuvad koostöös tellijaga tehtud otsusele, et kõik vastused rollide olemasolu kohta antakse päringu tegemise hetke seisuga ning lahendus ei pea vastama küsimusele minevikus kehtinud rollide kohta. Keskse pääsuhalduse lahenduse poolt pakutavad ja tarbitavad liidesed on rohkemas detailsuses kirjeldatud rajadokumendis.[11]

Kuna pääsuhalduse süsteem kui tervik ei toeta mitte konkreetset äriprotsessi vaid võimaldab eri osapooltel realiseerida nende äriprotsesse, ei ole käesolevas dokumendis kirjeldatud ei lõppkasutaja ega ka süsteemi teenindava ametniku läbitavaid äriprotsesse. Viimase osas sisaldab rajadokument nõudeid protsessidele kuid nende detailne analüüs on väljaspool käesoleva dokumendi ulatust.

Lahenduse realiseeritavad kasutuslood võib jagada kas kasutajate (lõppkasutaja, süsteem, taimer jne.) või skoobi (kasutuslood, milleta terviklik lahendus ei toimi ning teised) alusel. Loetavuse eesmärgil on joonised Joonis 1 ja Joonis 2 jagatud kasutajate alusel.

[10] Vt p 6.2.9
[11] Vt p 6.



Joonis 2. Keskse pääsuhalduse lahenduse süsteemi kasutuslood

Lisaks funktsionaalsetele nõuetele on lahendusele püstitatud ka rida mittefunktsionaalseid nõudeid. Nende aluseks on peamiselt arusaam, et klientsüsteemid on reeglina loodud ohutult tõrkuma, takistades lõppkasutajale mistahes teenuste kasutamise, kuni tema vastavaid õigusi ei ole võimalik kontrollida. Seega tähendab keskse pääsuhaldussüsteemi rike kõigi temast sõltuvate infosüsteemide riket. Ja kuna lahenduse loomise eesmärgiks on selle võimalikult lai kasutamine, võib keskse pääsuhalduse lahenduse tõrge viia laiaulatuslike tõrgeteni kogu riigi infosüsteemis.

On dokumenteeritud rida üldisi mittefunktsionaalsed nõudeid keskse pääsuhalduse lahenduse realisatsioonile. Lisaks üldistele nõuetele eksisteerivad nõuded lahenduse konkreetsete infrastruktuuri või orgvara osiste või väliste lahendustega. Need nõuded on kirjeldatud rajadokumendis.[12] Süsteemi üldised nõuded on:

- Kõik server-server sisend- ja väljundliidesed peavad olema puhverdatud järjekordade abil. See tähendab, et mitte ühelgi hetkel ei oota ükski kasutaja teenindamisega tegelev lõim välise süsteemi toimingu lõppemist. See nõue tuleneb vajadusest tagada süsteemi kõrg-käideldavus ning tema kesksest rollist riigi infosüsteemis: ei keskse pääsuhalduse süsteemi ega temaga liidestatud süsteemide dünaamiliselt keerukal käitumisel ei tohi olla võimalik häirida kogu riigi infosüsteemi

[12] Vt p 6.

tööd. Järelikult peab keskse pääsuhalduse lahenduse ja teda ümbritseva ökosüsteemi vahel paiknema töökindel dünaamiline puhver järjekordade näol[13]

- Keskne pääsuhalduse lahendus peab ohutult tõrkuma. Ehk, mitte ükski süsteemi veasituatsioon ei tohi viia olukorrani, kus klientsüsteemid võimaldaksid autoriseerimata ligipääsu, kõik tehnilised tõrked, mis võivad kahtluse või tõrke korral[14] viia "jah" vastuseni ligipääsu lubamise osas, peavad viima kas "ei tea" või "ei" vastuseni
- Kõik muutused rollides peavad olema tagatud terviklusega ning seotavad konkreetse autoriseeritud allikaga

Lisaks keskse pääsuhalduse lahenduse spetsiifilistele mittefunktsionaalsetele nõuetele peab loodav tarkvara vastama ka RIA mittefunktsionaalsete nõuete[15] kehtivale versioonile ning dokumendile "Digiriigi ristfunktsionaalsed nõuded".[16]

4. Kontseptsioon

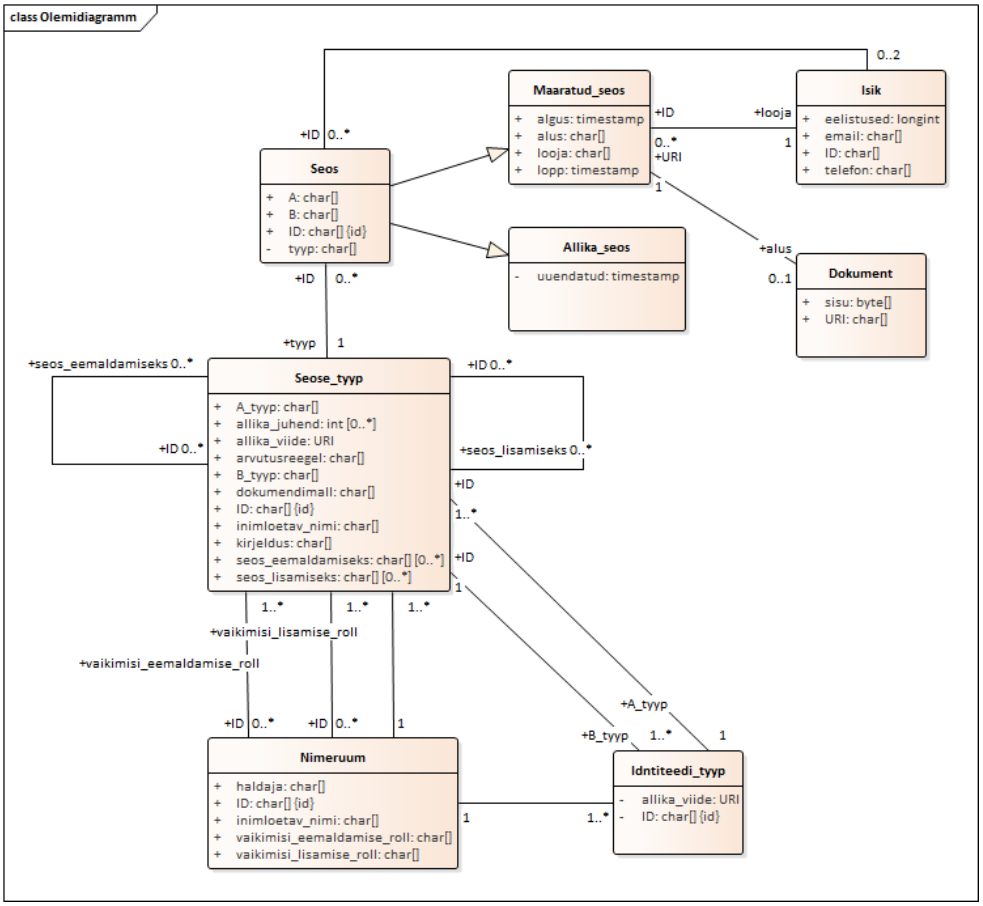
Kontseptuaalselt on pääsuhalduse lahenduse näol tegemist keskse toega võrgustikuga. See tähendab, et kuigi süsteemil on oluline ja keerulise tehnilise arhitektuuriga keskselt paigaldatav komponent, ei toimi süsteem tervikuna ilma suure hulga osapoolte - allikregistrite ja klientsüsteemide – koostööta.[17]

Seejuures on keskne pääsuhalduse lahendus olemuslikult tõepoolest võrgustikku toetav. Keskses pääsuhalduse lahendustes ei tehta ühtegi sisulist otsust ning tegeldakse ainult kas allikregistrite või lõppkasutaja poolt antud andmete hoidmise ja edastamisega. Pääsuhalduse lahendus ei tegele andmete tõlgendamisega. Nii see, mis alustel ja protsessi läbi kellelegi mingi roll (näiteks kas hooldaja eraisikute puhul või juhatuse liige juriidilise isiku puhul) tekib kui ka see, millised õigused sellest rollist tulenevad (näiteks õigus taotleda dokumenti või õigus esitada tollideklaratsioone), lahendatakse vastavalt allikregistrite ja klientsüsteemide poolt.

Kontseptuaalselt koosneb süsteem neljast suuremast osast:

[13] Näidet koos detailsema põhjendusega vaata p 7.3.
[14] Näiteks allikregistrite kättesaadavusprobleemide või ka näiteks vahemälu roiskumiseni viinud süsteemi sisemise rikke korral.
[15] https://e-gov.github.io/MFN/
[16] https://koodivaramu.eesti.ee/e-gov/cfr
[17] Sellise kontseptsioonini viinud disainiotsused on pikemalt kirjeldatud dokumendis „Tulevikulahenduse kirjeldus“.

- **Standardid ja kokkulepped**, mis määratlevad süsteemi koosvõime loovad talle hädavajaliku organisatoorse konteksti ja mida kirjeldavad käesoleva dokumendi punktid 5.4 ja 6.
- **Keskne pääsuhalduse lahendus**, mis realiseerib võrgustiku keskse toe ja mille kirjeldamisele keskendub suurem osa käesoleva dokumendi punktist 5.
- **Infosüsteemide tugi**, mis seisneb võrgustikku kuuluvate infosüsteemide poolt võrgustikule pakutavates ning sealt tarbitavates teenustes ning mida kirjeldab käesoleva dokumendi punkt 6.
- **Konfiguratsioon**, mis kirjeldab lahenduse poolt hallatavad pääsuõigused ning nende omadused ning mida kirjeldab käesoleva dokumendi punkt 5.3.



Joonis 3. Keskse pääsuhalduse lahenduse kontseptuaalne olemidiagramm

Süsteem kui tervik tegeleb järgmiste põhimõistetega, millede seosed on toodud joonisel Joonis 3:

- **Seos** ehk **roll** on seos kahe konkreetse objekti vahel. Seosed ei ole transitiivsed ehk pööratavad: väitest "A on B ema" ei tulene väide "B on A ema". Seosest "A on B ema" loogiliselt tulenev seos "B on A laps" tuleb sõnaselgelt määratleda. Seosed

jagunevad määratud seosteks, mida saab lisada ja eemaldada keskse pääsuhalduse lahenduse kaudu ja allika seosteks, millede allikaks on mõni allikregister. Iga määratud seosega on lisaks otspunktidele seotud ka viide selle loonud isikule.

- Kõik seosed kuuluvad mõnda **seose tüüpi**, mis kirjeldab seose omadused: seotavate objektide liigid (seos "A on B ema" on seos era- ja mitte juriidiliste isikute vahel), kas seose lisamine vajab elektroonilist allkirja, kas seos on muudetav jne.
- Kõik seose tüübid kuuluvad **nimeruumi**, mis koondab ühe funktsionaalse valdkonna seoseid ja võimaldab neid eristada teiste valdkondade omadest (seoste tüübid "finants#aruandja" ja "põllumajandus#aruandja" on erinevad). Samuti võimaldab nimeruum määratleda seoste tüüpide vaikimisi omadusi. Igal nimeruumil on üks ja ainult üks juriidilisest isikust haldaja
- Iga **isik** võib otse või oma esindaja vahendusel määrata oma kontaktandmed ning eelistused saadavate teavituste osas
- Iga määratud seosega võib olla seotud mõni **dokument**, millel on unikaalne URI ning mille sisu on kontseptuaalses mõttes struktureerimata baidijada

5. Vorm

5.1 Üldist

Lahenduse arhitektuuri vormi osa tuleneb ühest küljest realiseeritavast funktsionaalsusest ja kontseptuaalsetest valikutest selle funktsionaalsuse pakkumisel ning teisalt looval protsessil arhitektuurse lahenduse kirjeldamisel. Seega on allpool kirjeldatav lahendus tervikuna seotud nii pakutava funktsionaalsuse, konkreetse kontseptuaalse mõtteviisi kui arhitektuuri autoriga ning muutes ükskõik millist neist on tulemus erinev. Siiski joonistuvad välja kaks otsust, mis arhitektuuri vormi osa kriitiliselt mõjutavad:

- Kõik vastused rollide kohta antakse hetkeseisuga[18];
- Lahenduse taristus hoitakse kohalikku puhvermäluna toimivat koopiat väliselt määratletud seostest.

Nende otsuste muutmisel muutub olulisel määral nii konkreetsete komponentide realisatsioon kui ka süsteemi kui terviku struktuur. Samuti muutub lahenduse poolt pakutav võimalik teenustase ning selle parameetrid.[19]

[18] Vt p 3.
[19] Vt p 6.2.9.

5.2 Struktuur ja peamised komponendid

5.2.1 Ülevaade süsteemist

Järgnevas kirjeldatakse keskse pääsuhalduse lahenduse (ja mitte pääsuhalduse kui terviku) peamisi kõrge taseme komponente ning nende seoseid. Tegu on kontseptuaalse mudeliga, millele disaini faasis lisanduvad järjekorrad, koormusjaoturid API lüüsid jms. ning mille komponendid omakorda jagunevad tõenäoliselt mitmeteks tehnilisteks komponentideks. Näiteks Rollihalduri osana on tõenäoliselt mõistlik luua eraldi paigaldatav ja käitatav komponent, mis teavitab kasutajaid rollide aegumisest. Otsus, kas see komponent on eraldi paigaldatav, realiseeritud osana andmehoidlast või osana teenuskihist ei mõjuta lahenduse üldist arhitektuuri ning peaks olema seega tehtud lähtudes süsteemi käitavate ja realiseerivate inimeste kokkuleppest ja mitte arhitektuursetest kaalutlustest. Seejuures ei ole disaini faasis soovitav komponente ühendada või liita tehnilisi komponente kas osaliselt või kõikselt jagades. Nii võib toimida ainult juhul, kui käesolevas dokumendis kirjeldatud arhitektuur disaini faasis oluliselt muutub näiteks kontseptsiooni või funktsionaalsuse oluliste muutuste läbi.

Läbivalt kasutatav muster hoidla-adapter (Rollihaldur ja Muutmisadapter, Oraakel ja Oraakliadapter jt.) võimaldab eraldada liidese ja andmehoidla skaleerumisülesanded paigaldades halduri ja adapteri vahele järjekorra. Nii võib lisada kuitahes palju olekuta adaptereid kontrollides samas rangelt hoidlale rakendatavat koormust ning võimaldades pakutavate teenuse kontrollitud rikkeid.

Arhitektuurselt olulised ootused infrastruktuurile, sealhulgas näiteks kõigi haldur-komponentide osaks olevatele andmehoidlatele, on toodud punktis 6.2.10.

Komponendid on jaotatud primaarseteks ja sekundaarseteks selle järgi, kas keskne pääsuhalduse lahendus on ilma nendeta suuteline realiseerima primaarsed kasutuslood (Joonis 5) või mitte (Joonis 4).

Komponendid jagunevad oma rolli järgi neljaks:

- Komponendid, mille realiseerib mõni väline osapool väljaspool pääsuhalduse lahendust
- Komponendid, mis on osa pääsuhalduse tuumast
- Komponendid, mis tegelevad välistele osapooltele teenuste pakkumisega
- Komponendid, mis tarbivad väliste osapoolte teenuste tarbimisega

Selline liigitus võimaldab ühest küljest hinnata lahenduse eri komponentide sõltuvust välistest liidestest ja teisalt aitab teha disainiotsuseid nii tarkvara kui infrastruktuuri osas.

Mõlemal komponentdiagrammil on punktiirnoole semantika "sõltuvus": noole olemasolu komponendist A komponendini B tähendab, et komponent A sõltub oma põhifunktsiooni täitmisel komponendist B.

Lisaks allpool toodud lühikesele kirjeldusele komponendi funktsioonist kirjeldavad komponentide realiseeritavat funktsionaalsust rajadokumendi liideste osa[20], mis kirjeldab pakutavate ning tarbitavate liideste toimimist ning lisas 1, mis sisaldab seoseid kasutuslugude ja komponentide vahel.

5.2.2 Primaarsed komponendid

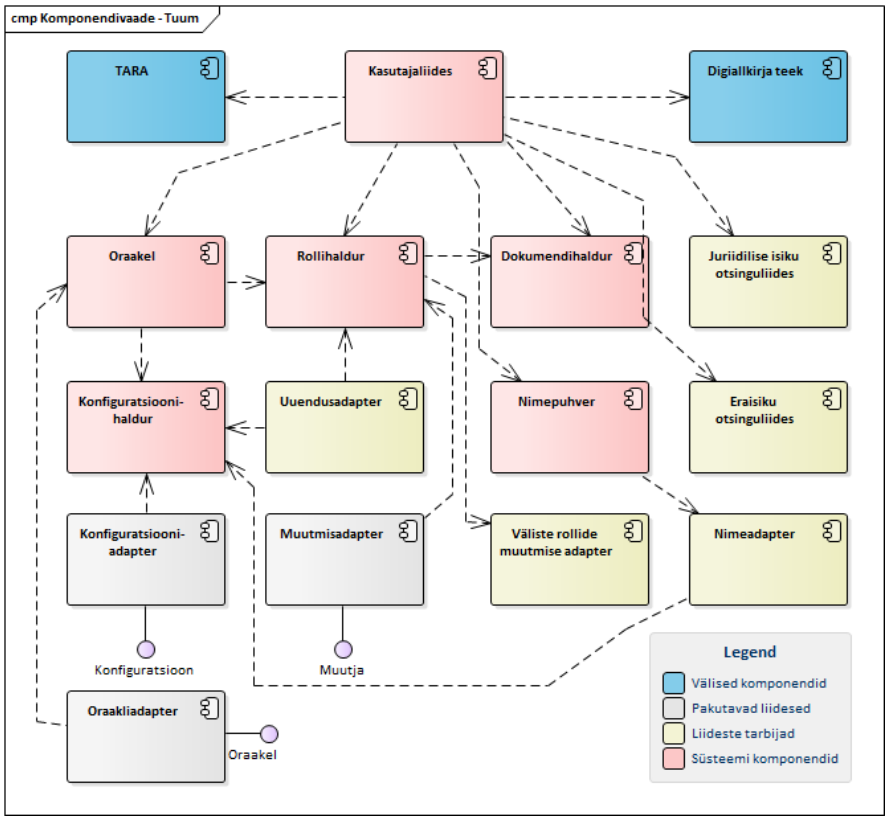
Primaarsed, ehk süsteemi tuumfunktsionaalsust pakkuvad, komponendid on järgmised:

- **TARA**. Standardne lahendus kasutajate tuvastamiseks;[21]
- **Digiallkirja teek**. Standardne lahendus kvalifitseeritud allkirja sisaldavate konteinerite loomiseks enimlevinud seadmete abil;[22.]
- **Kasutajaliides**. Realiseerib kogu lõppkasutajaga turvaliseks suhtlemiseks vajaliku funktsionaalsuse sisaldades kõiki selle funktsionaalsuse toimimiseks vajalikke varasid;
- **Oraakel**. Suudab konfiguratsiooni ja rollide andmestiku abil vastata päringutele rollide olemasolu või puudumise kohta;
- **Rollihaldur**. Sisaldab rollide andmestiku hoidmiseks, töötlemiseks (toimingud rollide algus- ja lõpukuupäevadel, rollide vahetused jne.) pärimiseks ja turvamiseks vajalikku funktsionaalsust;
- **Dokumendihaldur**. Sisaldab loogikat dokumendimallide alusel allkirjastatavate dokumentide loomiseks ning allkirjastatud dokumentide talletamiseks ning taasesitamiseks;
- **Juriidilise isiku otsinguliides**. Realiseerib side Kasutajaliidese ja äriregistri vahel juriidiliste isikute otsimiseks;
- **Eraisiku otsinguliides**. Realiseerib side Kasutajaliidese ja rahvastikuregistri vahel eraisikute otsimiseks;

[20] Vt p 6.
[21] Vt p 6.1.3.1.
[22] Vt p 6.1.3.2.

- **Konfiguratsioonihaldur**. Realiseerib funktsionaalsuse nimeruumide konfiguratsioonide salvestamiseks, muutmiseks ja versioneerimiseks ning suudab vastata küsimusele hetkel kehtivast konfiguratsioonist;
- **Uuendusadapter**. Vahendab allikregistrite muutusi konfiguratsiooni alusel Rollihaldurile;
- **Nimepuhver** on mittepüsiv mälupõhine vahemälu vältimaks liigseid päringuid identiteeti pakkuvate süsteemide suunas;
- **Nimeadapter**. Realiseerib funktsionaalsuse reaalajas nimede päringuks identiteeti pakkuvatest süsteemidest;
- **Konfiguratsiooniadapter**. Võimaldab ligipääsu Konfiguratsioonihaldurile ning realiseerib turvaserverist pärit andmete abil konfiguratsiooni pääsuhalduse loogika;
- **Muutmisadapter**. Võimaldab ligipääsu Rollihaldurile rollide muutmiseks masin-masin liidese kaudu;
- **Väliste rollide muutmise adapter.** Võimaldab rollihalduril pöörduda allikregistrite poole seal hoitavate rollide muutmiseks;[23]
- **Oraakliadapter**. Realiseerib funktsionaalsuse Oraaklile päringute esitamiseks;

[23] Kuigi muutus ise viiakse läbi Kasutajaliidese komponendis, on allikregistrites muutuste tegemise oluline aspekt ka nende kohaliku koopia võimalikult värskena hoidmine. Seetõttu ei pöördu Kasutajaliides mitte otse Väliste rollide muutmise adapteri poole vaid teeb seda Rollihalduri vahendusel.



Joonis 4. Keskse pääsuhalduse lahenduse peamised komponendid ja nende seosed

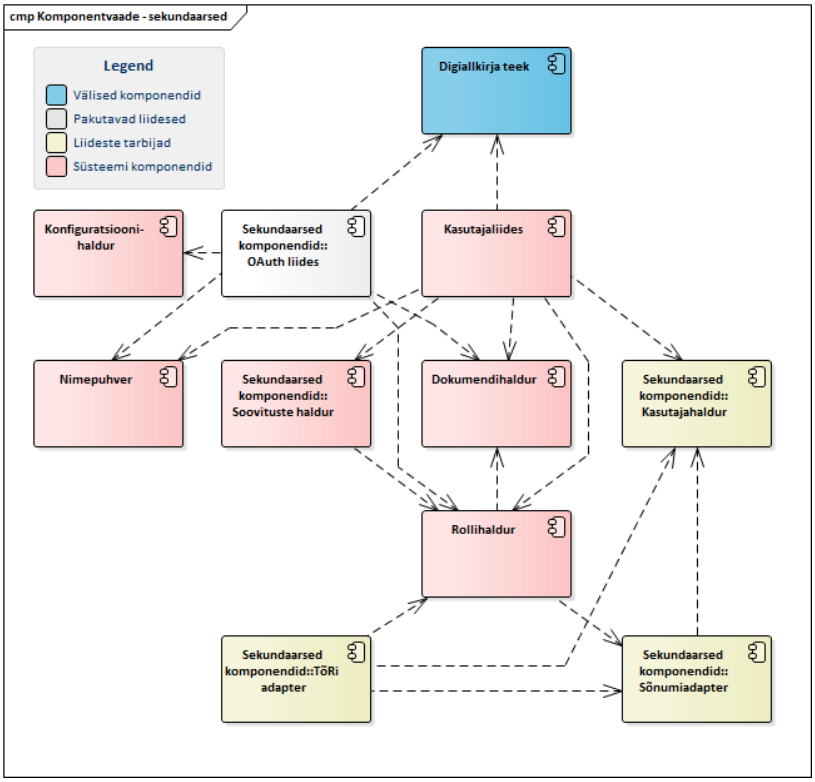
5.2.3 Sekundaarsed komponendid

Sekundaarsed komponendid on komponendid, mille lisamine suurendab kasutajamugavust, kuid ilma milleta on terviklahendus võimeline täitma oma peamist funktsiooni pääsuhaldust puudutava info kogumise jagamise näol. Joonis 5 kujutab lisaks sekundaarsetele komponentidele ka nende toimimiseks vajalikke primaarseid komponente.

- **OAuth liides**. Realiseerib liidesed välistele osapooltele OAuth voo abil rollide lisamiseks kasutaja nõusolekul;
- **Kasutajahaldur**. Realiseerib funktsionaalsuse kasutaja sõnumieelistuste talletamiseks ja pärimiseks ning väliselt osapoolelt kasutaja kontaktandmete talletamiseks ja pärimiseks;[24]
- **Soovituste haldur.** Realiseerib funktsionaalsuse soovituste andmiseks konkreetse rollikomplekti põhjal. Komponent on suuteline saama sisendina rea B-osapoole rolle ning väljastama viis sellise rollikomplektiga isikul suure tõenäosusega veel esinevat määratavat rolli järjestatuna tõenäosuse järgi;

[24] Vt p 6.1.3.9.

- **Sõnumiadapter**. Realiseerib suhtluse väliste osapooltega e-posti ja SMS sõnumite edastamiseks;[25]
- **TöRi adapter**. Realiseerib suhtluse töötamise registriga reageerimaks olukordadele, kus on kadunud isiku ja tema tööandja vaheline töösuhe kuid on alles nendevahelised seosed.



Joonis 5. Keskse pääsuhalduse lahenduse sekundaarsed komponendid ja nende seosed

5.3 Konfiguratsioon

Nimeruumide konfiguratsioon[26] on kriitiline osa keskse pääsuhalduse lahenduse arhitektuurist määratledes kõik tema kaudu kättesaadavad rollid, nende omavahelise suhted ning omadused[27].

[25] Kui sõnumite edastamiseks valitakse mõni muu kanal (näiteks eesti.ee postkast, millega liidestutakse mitte e-posti kaudu vaid otse), sõnumiadapteri olemus puhverdatud liidesena välise süsteemiga ei muutu
[26] Loomulikult on kesksel pääsuhalduse lahendusel, nagu kõigil teistel infosüsteemidel, ka tema sisemist toimimist ja struktuuri kirjeldav konfiguratsioon. Selle konfiguratsiooni struktuurile, käitlemisele ja haldamisele käesolev arhitektuur eraldi nõudeid ei püstita. Käesolevas dokumendis räägitakse konfiguratsioonist ja konfiguratsioonihaldusest eelkõige nimeruumide konfiguratsiooni kontekstis
[27] Seose mõiste ning omadused on pikemalt kirjeldatud dokumendis "Tulevikulahenduse kirjeldus"

Iga nimeruumi konfiguratsiooni võib vaadelda kui eraldi dokumenti, mis standardiseeritud grammatikale tuginedes kirjeldab konkreetse nimeruumi struktuuri. Nimeruumi struktuuri elemendid on kirjeldatud joonisel Joonis 3.

Igal nimeruumil on rida omadusi (näiteks inimloetav nimi ning vaikimisi vajalikud rollid rollide lisamiseks ja eemaldamiseks), ta sisaldab vähemalt ühte seose kirjeldust ning võib sisaldada identiteedi kirjeldusi. Seose kirjeldus määratleb seosega haaratud identiteetide tüübid ning seose allika: seos võib olla määratletud mõnes allikregistris, olla hallatav keskse kasutajaliidese kaudu, olla arvutatav teiste rollide alusel või moodustuda ühendina kõigist kolmest.

Arvutatavate rollide puhul moodustub seosesse kuuluvate isikute hulk hulgateoreetiliste tehete kaudu. Näiteks võib roll "aruandja" moodustuda rollide "juhatuse liige" ja "raamatupidaja" ühisosast sest mõlemasse hulka kuuluvatel isikutel on õigus ettevõtte nimel aruandeid esitada. Lubatud on vähemalt hulkade ühend, ühisosa, täiend ja vahe. Tehetes võib kasutada teisi arvutatavaid rolle. Rekursioon, kus rollid võivad sõltuda iseendast, ei ole lubatud.

On oluline mõista, et ka süntaktiliselt korrektne konfiguratsioon võib põhjustada süsteemi tõrkeid. Näiteks võivad liiga keerulised või andmemahukad arvutatavad rollid viia süsteemi komponentide ülekoormusele, sagedasti kasutatud rollide äkiline kadumine konfiguratsioonist viib klientsüsteemide tõrgeteni, viited integreerimata allikregistritele põhjustab ligipääsu kadu klientsüsteemides jne. Sedalaadi vead ei ole tehniliste vahenditega tuvastatavad ning seetõttu on konfiguratsioonihalduse protsess[28] keskse pääsuhalduse lahenduse puhul kriitilise tähtsusega.

Konfiguratsioonis on kõik inimloetavad rollide ja nimeruumide kirjeldused toodud ära lokaliseerituna. Konfiguratsioon ise kasutab Unicode standardit.

5.4 Standardid

Et lahenduse elemendid võiksid toimida tervikliku süsteemina, on hädavajalik kehtestada osapoolte vahel tehnilised standardid. Nii on võimalik, et klientsüsteemid ja allikregistrid ning keskne pääsuhalduse lahendus arenevad omasoodu olles siiski koosvõimelised. Standardid tuleb luua lahenduse loomise käigus, soovitavalt disaini faasis.

Standardiseerida tuleb vähemalt järgmised lahenduse aspektid:

[28] Vt p 6.2.6

- **Konfiguratsiooni grammatika**, mis võimaldab osapooltel tegelda nende vastutuse all oleva nimeruumi osa juhtimisega. Standard peab lisaks konfiguratsiooni kirjeldamise keelele määratlema ka kolmiku A:B:X esitamise grammatika ning identifikaatori grammatika, mida mõlemat kasutatakse lisaks konfiguratsiooni kirjeldamisele ka liidestes;
- Liidesed[29], mis võimaldavad osapooltel nii üksteisega kui keskse lahendusega suhelda:
  - **Oraakli liides**, mis võimaldab esitada päringuid seoste kohta;
  - **Muutja liides**, mis võimaldab seoseid muuta ja lisada;
  - **Nime liides**, mis võimaldab Nimeadapteril esitada päringuid identiteetide inimloetavate nimede kohta;
  - **OAuth liides,** mis võimaldab algatada rolli lisamist OAuth protokolli abil;
  - **Tookeni liides**, mis võimaldab tookeni abil rolle lisada;
  - **Allika liides,** mis võimaldab Uuendusadapteril pärida allikregistritest värsket informatsiooni seoste kohta.

6. Rajadokument

6.1 Tarkvara

6.1.1 Üldist

Tarkvara mõttes kirjeldab süsteemi rajadokument süsteemi poolt pakutavaid ja tarbitavaid liideseid, nende üldist funktsionaalsust, eeldusi ja kõrge taseme nõudeid kolmandatele osapooltele. Liideseid pakkuvaid komponente ning nende omavahelisi seoseid kujutab Joonis 4. Rajadokumendi eesmärk on süstemaatiliselt kirjeldada kõiki viise, kuidas lahenduse teda ümbritseva keskkonnaga suhestub.

Kõikide kirjeldatud server-server liideste puhul on eeldatud x-tee kasutamist tagamaks järgmist funktsionaalsust:

- Otspunktide tuvastamine nii, et kommunikatsioon toimub ainult kindlalt määratud osapoolte vahel
- Side terviklus on tagatud nii, et kõik sõnumid jõuavad muutmata kujul sihtpunkti
- Kõik päringud on logitud nii, et andmesubjektil on selge ülevaade tema andmete jagamisest osapoolte vahel

[29] Vt p 6.

- Päringud ei ole eitatavad nii, et ei päringu esitajal ega ka vastuse saatjal ei ole võimalik ei esitatud küsimust ega antud vastust eitada

Lisaks eeltoodule, peavad Konfiguratsiooniadapter, Muutmisadapter ja Oauth liides olema suutelised koos x-tee kaudu esitatud päringuga saama ka päringu esitanud osapoole identiteedi ning tagama, et konfiguratsiooni muutusi ning rollide lisamist ja eemaldamist saavad läbi viia ainult selleks autoriseeritud osapooled[30]. Kui toodud eeldused liideste puhul täidetud ei ole (näiteks kasutatakse mõnda muud sidelahendust, ei rakendata Andmejälgijat vms.), ei saa süsteem talle püstitatud eesmärke täita.

X-tee liideste stiil, st. kas REST või SOAP teenuste kasutamine, ei ole arhitektuurselt oluline.

Kui allpool on öeldud, et liides on x-tee kontekstis avalik, siis tähendab see, et sellele võib anda ligipääsu kõigile x-teega liitunud ning vastavad formaalsused läbinud osapoolele.

Kõik server-server sisend- ja väljundliidesed oleksid puhverdatud järjekordade abil[31]. Tarbitavatest liidestest on vaid otsingu ja nimeliidesed olemuselt sünkroonsed. Pakutavatest liidestest on sünkroonsed Kasutajaliides ja Oraakel.

Kõik keskse pääsuhalduse lahenduse piire ületavad kas sisenevad või väljuvad päringud peavad omama unikaalset identifikaatorit, mis edastatakse kõikidele kas päringule vastavatele või päringut ette valmistavatele ning vastust töötlevatele osapooltele.

Muud keskse pääsuhalduse lahenduse liideste realisatsiooni detailid ei ole arhitektuurselt kriitilised ning otsustatakse lahenduse disaini käigus.

Kõigi pakutavate liideste puhul on võimalikud (ja tuleb klientsüsteemi poolt käsitleda) järgmised tõrkestsenaariumid:

- Keskne pääsuhalduse süsteem ei ole x-tee turvaserveri kaudu kättesaadav. Näiteks on katkenud internetiühendus või ei toimi x-tee turvaserver;
- Keskne pääsuhalduse süsteem ei suuda päringutele teenustasemele vastava aja jooksul vastata. Näiteks on süsteem üle koormatud;
- Keskne pääsuhalduse süsteem ei suuda päringutele vastata. Näiteks põhjustab teatud päringutele vastuse koostamine mõne kaasatud komponendi katastroofilise hävingu.

[30] Eeldab kaitstud sidet nimetatud komponentide ja x-tee turvaserveri vahel
[31] Mõõnduse võib teha tarbitavate sünkroonsete liideste jaoks: kasutajakogemus on arhitektuurinõuete suhtes ülimuslik.

6.1.2 Pakutavad liidesed

6.1.2.1 Konfiguratsioon

Liidest pakub Konfiguratsiooniadapter. Konfiguratsiooni liides on viis süsteemi nimeruumide konfiguratsiooni pärimiseks ja muutmiseks. Kuna nimeruumide konfiguratsioon on süsteemi toimimise mõttes keskse tähtsusega peab nimeruumide haldus toimuma läbi rangelt kontrollitud ja hästi määratletud turvaomadustega kanali.

Liides on x-tee kontekstis avalik päringuteks kuid piiratud juurdepääsuga konfiguratsiooni muutmiseks.

Liides pakub järgmist funktsionaalsust:

- **Vaata konfiguratsiooni**. Tagastab konkreetse nimeruumi konfiguratsioonifaili sisu, selle kehtivuse algusaja, versiooninumbri ning järgmise oodatava konfiguratsioonimuutuse aja (kui on)
- **Muuda konfiguratsiooni**. Saab parameetriks nimeruumi viite, uue konfiguratsiooni kehtima hakkamise ajamärgendi ning konfiguratsioonifaili. Eduka päringu tulemusena hakkab antud ajamärgendil antud nimeruumi jaoks kehtima uus konfiguratsioon ning konfiguratsiooni vaatamise päring hakkab tagastama infot tulevase konfiguratsioonimuutuse kohta

Liidese kas kontrollitud või kontrollimatu tõrke korral tuleb konfiguratsiooni muutmise päring uuesti sooritada. Kestva tõrke korral võib konfiguratsiooni uuendamiseks kasutada manuaalset protsessi.[32] Tõrkestsenaariumid on järgmised:

- Päringu esitajal puudub õigus konkreetse nimeruumi konfiguratsiooni muutmiseks;
- Konfiguratsiooni kehtima hakkamise aeg ei ole piisavalt kauges tulevikus;
- Konfiguratsioonis esineb sisulisi vigu. Näiteks:
    - Konfiguratsioon ei ole süntaktiliselt õige;
    - Arvutatavad rollid tekitavad rekursiooni (rolli X kirjeldus viitab rolli Y kirjeldusele, mis viitab rolli X kirjeldusele).

6.1.2.2 Muutja

Liidest pakub Muutmisadapter. Muutja liides võimaldab lisada ja eemaldada konfiguratsioonis kirjeldatud seoseid olemite vahel. Tegu on samaaegselt nii tarbitava kui pakutava liidesega, sest seda võib lisaks kesksele pääsuhalduse lahendusele pakkuda ka

[32] Vt p 6.2.6.

mõni klientsüsteemidest. Kui liidest pakub keskne pääsuhalduse lahendus, kasutatakse teda keskse lahenduse poolt hallatavate rollide juhtimiseks klientsüsteemide poolt või selleks autoriseeritud osapoolte poolt[33] neid puudutavate seoste lisamiseks ja eemaldamiseks. Kui liidest pakub mõni klientsüsteemidest, kasutab seda kas keskne pääsuhalduslahendus või mõni muu autoriseeritud infosüsteem klientsüsteemi pääsuõiguste juhtimiseks. Sel juhul peab klientsüsteem olema kirjeldatud kui alliksüsteem.

Liides on x-tee kontekstis avalik, kuid rakendab sisemist õiguste kontrolli. Operatsioonid seosega on keskse pääsuhalduse poolt pakutavas liideses lubatud osapooltele, kes:

- On osapool A. Ehk, osapooled tohivad lisada endaga seotud rolle;
- On konfiguratsioonis kirjeldatud, kui alliksüsteem seosele X.

Liides pakub järgmist funktsionaalsust:

- **Lisa seos A:B:X.** Lisab seose X olemite A ja B vahele. Kui seos on juba olemas, kirjutatakse see üle ning lisamisoperatsioon lõpeb edukalt. Seejuures võib liides tagastada info üle kirjutamise fakti kohta;[34]
- **Eemalda seos A:B:X.** Eemaldab seose X olemite A ja B vahel. Seose puudumisel lõpeb operatsioon edukalt.

Liidese tõrkestsenaariumid on järgmised:

- Päringu esitajal puudub õigus rolli lisada või eemaldada;
- Lisatav roll ei ole konfiguratsioonis kirjeldatud.

6.1.2.3 Oraakel

Liidest pakub Oraakliadapter. Oraakli liides on peamine viis, kuidas klientsüsteemid keskse pääsuhalduse lahendusega suhestuvad. Liides on nimetatud nii, sest siitkaudu jõuab klientsüsteemideni puhas ilustamata tõde. Liides on standardne, ning seda võivad pakkuda ka allikregistrid. Nii tekiks võimalus kas püsivalt või ajutiselt klientsüsteemide päringud kesksest lahendusest eemale suunata vähendades nii viimase koormust ning parandades süsteemi kui terviku toimepidevust.

Liides on x-tee kontekstis avalik, päringuid võivad esitada kõik x-teega liitunud osapooled. Liides tagastab vastuse viimase parima teadmise alusel.

[33] Vt p 7.2.2.
[34] Kuigi seos kui selline operatsiooni käigus ei muutu, võivad muutuda seoste algus- ja lõpukuupäevad, mille muutusel võivad olla äriprotsessi jaoks olulised tagajärjed

Liides võimaldab esitada järgmisi päringuid:

- ***:B:X.** Tagastab vastuse küsimusele "milliste olemitega on antud identiteet antud seoses?";
- **A:*:X.** Tagastab vastuse küsimusele "millised olemid on antud identiteediga antud seoses?";
- **A:B:X.** Tagastab vastuse küsimusele "kas antud olem on teise antud olemiga antud seoses?".

Liidese kas kontrollitud või kontrollimatu tõrke korral tuleb eeldada, et kasutajal vastav roll puudub.

Tõrkestsenaariumid on järgmised:

- Keskse pääsuhalduse süsteemi sisemine olek ei võimalda anda päringule teenustasemele vastavat vastust. Liides tagastab vastava veakoodi. Näiteks ei ole Uuendusadapter suutnud piisava aja jooksul mõnest allikregistrist andmeid pärida.

6.1.2.4 Kasutajaliides

Liidest pakub komponent Kasutajaliides. Keskse pääsuhalduse lahenduse kasutajaliides tegeleb ainsana pakutavatest liidestest lõppkasutajale teenuste pakkumisega. Kasutajaliidest kui kasutajaga suhtlemise viisi kirjeldab pääsuhalduse lahenduse prototüüp koos kaasneva dokumentatsiooniga. Liides ei sisalda avalikult, ilma kasutajat tuvastamata, kasutatavat funktsionaalsust.

6.1.2.5 OAuth liides

Liidest pakub komponent "OAuth liides". Liides pakub OAuth 2.0 standardi voogu Authorization Code Flow[35], mis lõpeb kliendile[36] autoriseerimiskoodi väljastamisega. Kuigi sama funktsionaalsust saab realiseerida ka standardeid kasutamata ning antud juhul ei kasutata ära kõiki OAuth standardi võimalusi, võimaldab standardi kasutamine lihtsamat suhtlust integratsioonipartnerite vahel, vähendab tehniliste otsuste hulka ning võimaldab kasutada ennast tõestanud tarkvarateeke.

Liides ootab Authorization Request päringus väljas:

[35] RFC 6749 punkt 4.1
[36] OAuth liidest kirjeldavas lõigus kasutatakse RFC 6749 mõisteid, muu hulgas tähendab mõiste "klient" autoriseerimisprotsessi algatanud osapoolt

- `client_id` seose A-osapoole identifikaatorit standardses formaadis; [37]
- `scope` tühikutega eraldatud nimekirja lisatavate rollide identifikaatoritest.

Pärast autentimist kuvatakse ressursiomanikule küsitud rollide nimekiri koos küsiva identiteedi (saadakse väljast `client_id`) masinloetava nimega ning antakse võimalus valida, milliseid rolle ta anda soovib. Konfiguratsioonis mitte leiduvaid rolle ei kuvata.

Access Token Response sisaldab alati väljas:

- `scope` kasutaja poolt tegelikult valitud rollide identifikaatorite tühikutega eraldatud nimekirja;
- `token_type` stringi "bearer";
- `access_token` JWT (RFC 7519) tookenit krüpteeritud vastavalt JWE (RFC 7516) standardile. Täpne krüpteerimisalgoritmi ja selle parameetrite toimub disaini faasis, valik sõltub realisatsiooni hetkel saada olevast parimast teadmisest ning eelistustest võtmehalduse protseduuride (vt p 6.2.11) osas. Tookenisse lisatakse
    - sama välja `scope` väärtus, mis tagastatakse ka lahtise tekstina;
    - voo algatanud osapoole (A-osapool) identifikaator standardses formaadis;
    - protsessi käigus sisse loginud kasutaja identifikaator (B-osapool) standardses formaadis;
    - tookeni kehtivuse lõpp.

Võib tekkida olukord, kus kasutaja eemaldab antud volitused ning klient need tookenit kasutades taastab. Sellise olukorra vältimiseks peab tookeni eluiga olema lühike, suurusjärgus mõned minutid. Nii on küll kasutaja ümber mõtlemine põhimõtteliselt võimalik kuid ebatõenäoline. Jääkriski maandamiseks võib realiseerida tookeni ühekordse kasutuse reegli kuid lisanduv keerukus ei tasu ennast tõenäoliselt ära. Ühekordse tookenite realisatsiooni puhul tekib vajadus eraldi tookenite puhvri järele, mis on OAuth liidese instantside vahel jagatud. Lisaks tekib komakorda lahendamist vajav võimalus OAuth liidese ja kliendi vahelise oleku ebakõlaks, kui viimane näiteks ei saa kätte tookeni liidese vastust: tooken on küll juba kasutatud, kuid kliendil puudub võimalus sellest teada saada.

6.1.2.6 Tookeni liides

Liidest pakub komponent "Oauth liides". Tookeni liides on x-tee liides rollide lisamiseks Oauth voo käigus väljastatud pääsutookeni alusel. Liides ei ole standardne.

[37] Vt p 5.4.

Liides on x-tee kontekstis avalik, päringuid võivad esitada kõik x-teega liitunud osapooled.

Liides võimaldab esitada järgmisi päringuid:

- **Lisa roll**. Päring saab parameetriteks soovitava B-osapoole identifikaatori standardses formaadis ja eelnevalt väljastatud juurdepääsutookeni. Tookeni sobivuse korral lisatakse selles leiduvad rollid.

Tõrke korral tuleb eeldada, et rolle ei lisatud.

Tõrkestsenaariumid on järgmised:

- Tooken ei ole sobiv antud päringu läbi viimiseks (tagastatakse vastav veakood), pole täidetud järgmised tingimused:
    - tooken on krüptograafiliselt valiidne (st. kas teda õnnestub avada);
    - tooken on veel kehtiv;
    - tookenis sisalduv A-osapoole identiteet ühtib päringu teinud x-tee osapoole identiteediga
    - tookenis sisalduv ja liidese parameetrina saadetud B-osapoole identiteet ühtivad.
- Viidatud rollidest mõnda ei eksisteeri enam konfiguratsioonis või ei ole see sobiv soovitud identiteetide tüüpidele

6.1.3 Tarbitavad liidesed

6.1.3.1 Autentimine

Kuna keskne pääsuhalduse süsteem ei tegele osapoole identiteetidega, ei ole tema skoobis ka lõppkasutaja tuvastamine. Selleks tarbeks kasutatakse standardset lahendust, näiteks TARA, mis võimaldab tuvastada nii Eesti kui välisriikide kodanikke. Seejuures võtab keskne pääsuhalduse lahendus identiteedi mõttes agnostilise rolli: millise iganes identiteedi TARA lahendusele suunab, seda käsitletakse kui standardset isiku identiteeti ning käivituvad samad päringud, mis Eesti isikukoodiga kasutajagi puhul. Kui leidub allikregistreid, kus tuvastatud kasutajale on määratud rolle, need ka kuvatakse.

6.1.3.2 Digiallkirja süsteem

Digiallkirja süsteem integreerub brauseri vahendusel kasutajaliidesega ning võimaldab kasutajal allkirjastada dokumente kasutades enamlevinuid kvalifitseeritud allkirja

vahendeid, näiteks ID-kaart, mobiili-ID ja SmartID. Juhul, kui sellise võimekusega lahendust ei ole[38], tuleb see luua ning pääsuhalduse lahendusega liidestada.

6.1.3.3 Muutja

Kui konfiguratsioonis on roll märgitud samaaegselt kasutajaliideses muudetavaks ja varustatud allikregistri viitega, kasutab keskne pääsuhalduse lahendus Muutja liidest, et kasutaja valikud rollide lisamisel ja eemaldamisel allkiregistrile teatavaks teha. Seejuures eeldatakse, et realiseeritud on Muutja liides täpselt samal standardsel kujul, nagu seda pakub keskne pääsuhalduse süsteem.[39]

6.1.3.4 Nimeadapter

Nimeadapteri tarbitav Nimeliides võimaldab kasutajaliidesel läbi lühikese elueaga nimepuhvri pärida identiteedi allikalt objektide inimloetavaid nimesid. Kui vastavat objekti identifitseerivat inimloetavat nime puhvrist ei leita, pöördutakse läbi nimeadapteri konfiguratsioonis määratud süsteemi - identiteedi allika - poole nime leidmiseks. Tüüpiliselt on selleks mõni alliksüsteem, näiteks tuleb tõenäoliselt inimeste nimesid pärida rahvastikuregistrist ja ettevõtete omi äriregistrist.

Identiteedi allikas realiseerib standardse Nime liidese, mis saab sisendiks standardse identifikaatori ning väljastab Unicode teksti. Seejuures on identiteedi allikas vastutav väljastatava inimloetava nimekuju ohutuse eest.[40]

6.1.3.5 Otsinguliidesed

Otsinguliidesed võimaldavad kasutajal kasutajaliidese vahendusel otsida kas juriidilisi- või eraisikuid. Kuna liidesed peavad olema suure jõudlusega ning tõrkekindlad tagades samal ajal mugava kasutajakogemuse ning kaitstes kasutajate privaatsust, on ilmselt tegu keerulise, paljusid eri organisatsioonidesse kuuluvaid osapooli hõlmava, kompromissiga. Seetõttu tuleb liideste realisatsiooni detailid kokku leppida läbirääkimistes äri- ja rahvastikuregistriga. Kuigi eelistatud on standardne x-tee liides, ei ole sobiva tehnilise

[38] Dokumendi loomise hetkel ei ole selge, kas ja mil määral olemasolevad süsteemid (sealhulgas SIGa, https://github.com/open-eid/SiGa) keskse pääsuhalduse lahenduse vajadusi rahuldavad.
[39] Vt p 6.1.2.2.
[40] Kuna nime kuvatakse kasutajale turvalises brauseri kontekstis, võib pahatahtlik nimi muu hulgas sisaldada ka käivitatavat koodi viies nii ellu XSS ründe.

lahenduse olemasolul ja latentsi vähendamise eesmärgil välistatud ka otsingupäringute sooritamine otse brauserist konkreetse infosüsteemi pakutavate liideste vastu.

Sõltumata realisatsioonist peavad otsinguliidesed tagama andmesubjektide õiguste kaitse ning takistama otsitava registri täielist kopeerimist automatiseeritud liidese abil. Selleks peavad liidese mõlemal pool, nii keskse pääsuhalduse lahenduse kui liidest pakkuva süsteemi juures, olema realiseeritud

- Liidese väärkasutust takistav äriloogika (piirangud tagastavate kirjete arvule, piirangud korrutus-otsingu[41] takistamiseks jne.);
- Kiiruskontrollid, mis piiravad liidese suunas esitatavate päringute hulka;
- Monitooringuvahendid, mis võimaldavad väärkasutust tuvastada ning intsidente menetleda.

Meetmete realisatsioon mõlemal pool tagab ühelt poolt sujuva kasutajakogemuse ning teisalt kaitse nii kasutajaliidesest kui ka serveri kompromiteerimisest tulenevate rünnete vastu.

6.1.3.6 Sõnumiliidesed

Keskne pääsuhalduse lahendus teavitab kasutajaid, vastavalt nende eelistusele, kas elektronposti või SMS sõnumite teel. Kuna sõnumite edastamine on süsteemis selgelt eraldatud sündmuste tekkimisest, võib edaspidi lisada milliseid iganes sõnumite edastamise kanaleid, näiteks ka standarditud x-tee liideste näol.

Kuna kasutaja teavitamine ei ole keskse pääsuhalduse lahenduse tuumfunktsionaalsus[42], pole otstarbekas realiseerida kõiki eri kanalitesse sõnumite edastamise keerukust katvaid kasutuslugusid nagu tagasi põrkavad kirjad, telefoninumbrite valideerimine jms. Seetõttu eeldab keskne pääsuhalduse lahendus sõnumite saatmiseks liidestust mõne teenusepakkuja infosüsteemiga, kus liidese semantikaks on adressaat ja sõnumi sisu ning kus ülejäänu eest hoolitseb teenusepakkuja.

[41] Rünne, kus korduvate otsingupäringute abil saadud tulemusi omavahel võrreldes tuletatakse objekti varjatud omadus: kui kirje esineb otsingutulemustes nii "A ja B" kui "B ja C" otsingute puhul, võib tal järeldada olevat omadus B isegi, kui üksik otsing seda omadust varjab.
[42] Vt „Kasutuslugude ja prototüübi kirjeldus“p 1.

6.1.3.7 Uuendusadapter

Uuendusadapter vastutab selle eest, et keskse pääsuhalduslahenduse sisemine koopia väljaspool kirjeldatud seostest oleks adekvaatne. Selleks on kaks võimalust:

- Kasutatakse Allika liidest, mis laiendab Oraakli liidest päringuga *:*:X võimaldades alla laadida kõik alliksüsteemile teada olevad seosed. Vastava võimekusega adapter käivitub perioodiliselt, loeb konfiguratsioonist uuendatavate allikate andmed, käivitab vastavad päringud ning salvestab tulemused;
- Kasutades allikaspetsiifilist integratsiooni, kus alliksüsteem näiteks teavitab muutustest üksikute sõnumitega, võimaldab perioodiliselt alla laadida registri muutuste nimekirja vms.

Kuna lisaks standardsele liidesele on integratsiooniks ka muid võimalusi, sealhulgas passiivseid, võib uuendusadapter olla realiseerituna mitme erineva tehnilise komponendina.

6.1.3.8 Tõlge

Kuigi tõlke puhul pole käesolevas arhitektuuris tegemist masin-masin ega masin-kasutaja liidesega, tarbib süsteem siiski eeldatavasti välise osapoole poolt loodud tõlkefaile, mis moodustavadki tõlke liidese. Tõlkefaile vajavad järgmised komponendid:

- **Kasutajaliides**, mille kõik kasutajale kuvatavad sõned, sealhulgas konfiguratsioonis sisalduvad rollide masinloetavad nimed ja muud toetavad tekstid, on tõlgitavad;
- **Sõnumiadapter**, mille kõik kasutajale saadetavate sõnumite mallid on tõlgitavad.

6.1.3.9 Kasutajate kontaktandmed

Süsteemi funktsionaalse skoobi määratlemisel on otsustatud, et kuigi kasutaja saab keskses pääsuhalduse lahenduses juhtida oma eelistusi selles osas, mis sündmuste puhul mis kanalisse kasutaja teavitusi saada soovib, juhitakse kasutaja kontaktandmeid siiski süsteemiväliselt. Nii saab tagada, et kasutaja ei pea tema jaoks ühe rakenduse, eesti.ee, eri osades erinevaid kontaktandmeid määrama.

Järelikult peab leiduma väline liides, mis, saades sisendiks isikukoodi, suudab tagastada telefoninumbri ja e-maili aadressi.

6.2 Orgvara

6.2.1 Üldist

Orgvaralised liidesed kirjeldavad süsteemi piire ületavaid või süsteemi oluliselt mõjutavaid äriprotsesse ja muid organisatsioonilisi elemente. Sisuliselt on tegemist organisatoorsete nõuete komplektiga, mis kirjeldab süsteemi vajadusi teda toetavate ja ümbritsevate äriprotsesside osas.

Süsteemi nõudeid juriidilise konteksti osas kirjeldab dokument „Õiguslik analüüs."

Allpool kirjeldatud protsesse on reeglina vaja toetada mingit liiki tehnilisi lahendusi, mis ei ole otseselt pääsuhalduse lahenduse osa. Samas, kuna ilma nendeta ei toimiks süsteemi jaoks olulised protsessid, on lahenduse vaatest siiski tegu oluliste süsteemidega. Seoseid orgvara ning neid toetavate tarkvaralahenduste vahel kirjeldab Tabel 1.

Tabel 1. Tugiprotsesside ja tarkvara seosed

	Kirjeldus	Standardne/erilahendus	Andmekaitse	Infoturve	Klienditugi	Klientsüsteemi liitumine	Konfiguratsiooni haldus	Monitooring	Teavituskanalite hooldus	Teenusehaldus	Lokaliseerimine	Võtmehaldus	Standardite haldus	Sõltuvuste haldus
Andmejälgija	Standardne andmejälgija	S	X											
Logide hoidmine ja analüüs	Lahendus eri komponentide logide kokku kogumiseks ja analüüsiks	S		X						X				
Klienditugi	Kliendi pöördumiste haldamine ja protsessi juhtimine	S			X	X				X				
Testkeskkond	Keskkond konfiguratsioonihalduse ja integratsioonide testimiseks	E					X							
MISP2	MISP2 ehk mini-infosüsteem-portaal on standardne X-tee valmiskomponent	S					X							
Monitooring	Süsteemi tervise jälgimine	S	X	X				X	X	X				
Lokaliseerimine	Kasutatavate tekstide tõlge	S									X			
Viki	Tekstide koosloome ja teadmusjuhtimine	S				X				X			X	X

	Kirjeldus	Standardne/erilahendus	Andmekaitse	Infoturve	Klienditugi	Klientsüsteemi liitumine	Konfiguratsiooni haldus	Monitooring	Teavituskanalite hooldus	Teenusehaldus	Lokaliseerimine	Võtmehaldus	Standardite haldus	Sõltuvuste haldus
Tervis	Võimalus kommunikeerida lahenduse ja selle osade tervist	E			X					X				
Võtmehaldus	Lahendus krüptomaterjali genereerimiseks											X		

6.2.2 Andmekaitse

Keskne pääsuhalduse lahendus on disainitud minimeerima tundlike isikuandmete töötlemist käideldes ainult olemuslikult hädavajalikke seoseid olemite vahel ning puhverdades lisainfot nagu inimloetavad nimed vaid lühiajaliselt. Siiski on tegu andmekaitse mõttes olulise süsteemiga ning tal on andmekaitse protsessile järgmised nõuded:

- Pakutavatele x-tee liidestele peab olema paigaldatud standardne Andmejälgija[43], mis on suuteline isikukoodide alusel päringutest ja nende vastustest lõppkasutajale mõistetava logi moodustama. Nii saab tagada, et kõik päringud süsteemi suunas muutuvad andmesubjektile jälgitavaks
- Kõik x-tee kaudu pakutavad ja tarbitavad liidesed peavad olema kaetud asjakohaste lepingutega ning vastama kehtivatele nõuetele;
- Tuleb tagada, et alliksüsteemide kaudu jagatav informatsioon andmesubjektide kohta vastaks süsteemi avalikkuse (kõik seosed on päritavad kõigi liitunud osapoolte poolt) eeldustele;
- Tuleb tagada, et sõnumiliideste kaudu kolmandate osapoolte vahendusel kasutajani liikunud info kaitse on tagatud kas tehniliste või juriidiliste meetmetega;
- Kõik isikuandmeid töötlevad hoidlad[44] ja infrastruktuuri poolt pakutav logilahendus[45] peavad olema nõuete kohaselt dokumenteeritud kas ühise pääsuhalduse andmekogu raames või eraldi andmekogudena;

[43] Eeldatakse, et tarbitavate liideste puhul vastutab andmejälgija paigaldamise eest liidest pakkuv osapool.
[44] Vt p 6.3.4.
[45] Vt p 6.3.6.

- Peab toimuma otsinguliideste kasutuse jälgimine tuvastamaks nende väärkasutust rahvastiku- ja äriregistri andmete volituseta töötlemiseks.

6.2.3 Infoturve

Nii kriitilise süsteemi nagu seda on keskne pääsuhalduse lahendus kaitseks peab olema rakendatud laiapõhjaline infoturbemeetmete komplekt. Kaks süsteemi toimimise mõttes kriitilist nõuet infoturbe protsessidele on:

- Kesksele pääsuhalduse lahendusele Eesti infoturbestandardi E-ITS rakendamine, sealhulgas kaitsetarbe taseme määramine ning sellest tulenevate meetmete rakendamine;
- Intsidendivaste, mis suudab efektiivselt tagada kõigi süsteemiga liidestunud osapoolte kaasamise intsidentide ära hoidmisse, tuvastamisse ning nende tagajärgedega tegelemisse.

6.2.4 Klienditugi

Funktsionaalselt tehnilise ja keeruka süsteemi, nagu seda on pääsuhalduse lahendus oluliseks tugisüsteemiks on klienditugi. Eristub kaks eraldi protsessi:

- Lõppkasutaja tugi, mis toetab kasutajat võimalike tekkivate probleemide lahendamisel nii süsteemi kasutamisel kui ka süsteemist tuleneva juurdepääsuga seotud probleemide (näiteks puudub ligipääs vajalikule funktsionaalsusele hoolimata kasutaja määramisest rolli) lahendamisel;
- Klientsüsteemi tugi, mis toetab klientsüsteemi nii tehniliste (näiteks konfiguratsioonihaldus) kui ka funktsionaalsete (näiteks klientsüsteemi klienditoe intsidendid) probleemide lahendamisel.

6.2.5 Klientsüsteemi liitumine

Et pääsuhalduse lahendus looks kliendile väärtust, peab temaga ühel või teisel viisil liidestunud olema võimalikult palju süsteeme. Seetõttu on oluline, et klientsüsteemi liidestumine oleks protsessina juhitud ning süsteemi operaatori poolt läbi kogu elutsükli ideest kuni tootekeskkonda paigalduseni toetatud. Tuleb arvestada ka klientsüsteemide erinevate vajadustega, mis ulatuvad täisintegratsiooni teed läinud suurtest riigi infosüsteemi elementidest erasektori ettevõteteni, kelle jaoks on pigem tegu sekundaarse

protsessi automatiseerimisega. Samuti tuleb arvestada, et aja jooksul väheneb klientsüsteemi liitumise protsessi olulisus ning tõuseb klientsüsteemi toe oma.

6.2.6 Konfiguratsiooni haldus

Kuna kogu pääsuhalduse lahenduse toimimine on kriitilises sõltuvuses nimeruumide konfiguratsioonist, on nimeruumide konfiguratsiooni haldus protsessina süsteemi toimimiseks ülioluline. Süsteemi vaatepunktist on oluline, et protsess täidaks järgmisi nõudeid:

- Eksisteerib alamprotsess, millega määratakse, eemaldatakse ja muudetakse organisatsioone, kes tohivad nimeruume hallata. Alamprotsessi eesmärgiks on tagada, et igal ajahetkel on igal nimeruumil konkreetne haldaja ning et see haldaja ei vahetuks ilma selgelt defineeritud ning juriidiliselt korrektse protsessita.
- Kuna süsteemi konfiguratsioon on keeruline süsteem iseeneses, siis on vajalik konfiguratsiooni testimisprotsessi loomine. Selleks tuleb tõenäoliselt kättesaadavaks teha eraldi testkeskkond, samuti võib vajalikuks osutuda eraldi konfiguratsiooniga seotud testraamistiku loomine, mis võimaldab näiteks arvutatavaid rolle väiksemamahulise andmestiku najal testida.
- Peab eksisteerima protsess, mis võimaldab konfiguratsiooni käsitsi uuendamist, kui uuendamine masinliidese kaudu ei ole kas võimalik või otstarbekas. Näiteks on käsitsi uuendamine tõenäoliselt otstarbekas kriisisituatsioonis ja olukorras, kus konfiguratsiooni haldab süsteemi operaator ise. Manuaalne konfiguratsiooni uuendamise protsess peab tagama samal tasemel auditeeritavuse ning terviklikkuse, kui konfiguratsiooni uuendamine masinliidese kaudu.
- Protsess peab tagama, et ka x-tee kaudu tulnud konfiguratsiooni uuendusele järgneks manuaalne protsess tagamaks, et allikregistrite integratsioon toimib, et osapooled saaksid uuendusest teada ning et uuendus ei too süsteemile kui tervikule kaasa soovimatuid tagajärgi. Just sel otstarbel on Konfiguratsiooni liidese kirjelduses sätestatud nõue, et konfiguratsiooni edastamise ja selle kehtima hakkamise vahele peab jääma piisav aeg.
- Peab eksisteerima koordineeritud tugi konfiguratsiooni muutustele. Kuna rolle võidakse kasutada rohkem kui ühes klientsüsteemis, on oluline koordineeriva funktsiooni olemasolu: Kui kaob roll, mida mõni klientsüsteem seda veel kasutab, ei pääse sellesse rolli määratud inimesed enam klientsüsteemi vastavat rolli vajavale funktsionaalsusele ligi. Mõistlik oleks näiteks muuta kaduv roll mingiks perioodiks

mittelisatavaks ja asendada aeglaselt uuega, vajalik võib olla rollihoidla uuendamine käsitsi ning kindlasti on vajalik koordineeritud kliendi-suunaline kommunikatsioon. Selleks kõigeks peab eksisteerima keskne koordineeriv funktsioon.

- Rollide nimekiri, kirjeldus ja omadused (sealhulgas allikregistritest päritud rollide oma) peab olema avalikult dokumenteeritud ja kättesaadav. Eriti oluline on kirjeldada peamiste allikregistrite nagu rahvastiku- ja äriregister rollide juriidiline sisu. Ehk, mis nõuete täidetusel väljastab allikregister seose konkreetsete isikute vahel.

6.2.7 Monitooring

Pääsuhalduse lahenduse näol on tegemist hajusa keskselt toetatud lahendusega, seetõttu sõltub süsteemi kui terviku toimimine väga paljudest osapooltest. Monitooringu protsessi ülesanne on tagada, et informatsioon oluliste liidestunud infosüsteemide olukorrast muutuks teadmiseks pääsuhalduse süsteemi kui terviku tervisest ning et huvitatud osapooled saaksid pädevat informatsiooni keskse pääsuhalduslahenduse olukorra kohta. Monitooringuinfo kogumiseks ja haldamiseks on süsteemi realisatsiooni käigus tõenäoliselt mõistlik luua keskne "terviseinfo" lehekülg[46], mis annaks infot süsteemi eri komponentide tervisest ning koondaks osapooltele suunatud monitooringuinfo ühte kohta.

Monitooringu protsess toetub suurel määral infrastruktuuri poolt pakutavale logide kogumise, haldamise ja analüüsimise võimekusele.[47]

6.2.8 Teavituskanalite hooldus

Kuna keskse pääsuhalduse lahenduse sekundaarne funktsionaalsus sõltub süsteemi võimest kasutajaid elektronposti ja SMS sõnumite teel teavitada, peab eksisteerima äriprotsess, mis vastava liidese olemasolu tagab. Selle protsessi käigus tagatakse vastavate lepingute olemasolu ja uuendamine, teenuse eest tasumine, reageerimine käideldavusintsidentidele, teenustaseme kontroll jne.

6.2.9 Teenusehaldus

Teenusehalduse protsessi eesmärk on tagada ühest küljest keskse pääsuhalduse lahenduse kui teenuse toimimine vastavalt selgelt kokku lepitud teenustasemele ja teisalt ka teenustaseme osapooltega kokku leppimine. Nii paljude osapooltega ja nii kriitilise

[46] Vt näiteks https://status.aws.amazon.com/.
[47] Vt p 6.3.6.

süsteemi toimepidevuse tagamiseks on oluline, et keskse lahenduse teenustaseme dokument (st. kirjeldus sellest, millisele tasemel pakutav teenus vastab) on avalik.

Keskse pääsuhalduse lahenduse toimimine on defineeritud kui olukord, kus lahendus suudab kättesaadavusnõuetele vastava aja jooksul korrektselt vastata küsimusele seose olemasolu või puudumise kohta tuginedes teenustasemes määratletud mõttes korrektsetele andmetele allikregistritest.

Teenustaseme dokument peab sätestama konkreetsed väärtused järgmistele süsteemi käitumise parameetritele:

- Kättesaadavus. a % päringutest peavad saama vastuse b millisekundi jooksul;
- Planeeritav taasteaeg. Süsteemi toimimine taastatakse c tunni jooksul pärast intsidenti;
- Andmekadu:
    - Toimingute aluseks olevad andmete muudatused võivad kaduda kõige rohkem d minuti ulatuses;
    - Toimingulogid võivad kaduda kõige rohkem e minuti ulatuses.
- Allikregistri fi muutused kajastuvad süsteemi vastustes mitte hiljem, kui gi tunni jooksul.

6.2.10 Lokaliseerimine

Keskse pääsuhalduse lahenduse suhtlus kasutajaga toimub erinevates keeltes. Seetõttu on vajalik protsess, mis tegeleb eri kasutajasuhtluse elementide tõlkimisega.

Tõlkimist vajavad järgmised suuremad elementide grupid:

- Kasutajaliides koos relevantsete abitekstidega;
- Sõnumiadapteri poolt saadetavad E-posti ja SMS sõnumid;
- Rollide inimloetavad kirjeldused ja muud konfiguratsioonis määratud kasutajale mõeldud tekstid.

Tuleb silmas pidada, et kui kasutajaliideses kasutatavad sõned ning sõnumite mallid on oma olemuselt staatilised ja tõenäoliselt väljaspool tarkvara tarneprotsessi ei muutu, siis konfiguratsioon ja seega ka tema inimloetavate osade tõlge võib muutuda pidevalt. Seetõttu on lokaliseerimisprotsess tihedalt seotud konfiguratsiooni halduse protsessiga.[48]

[48] Vt p 6.2.6.

6.2.11 Võtmehaldus

OAuth liides väljastab krüpteeritud tookeneid tagamaks, et x-tee kaudu saabunud päring on seotud konkreetse kasutaja poolt tehtud valikutega.[49] Krüpteerimise eesmärk on ühest küljest tagada tookenite terviklus kuid teisalt ka nende autentsus. Seetõttu peab OAuth liidese komponent omama ligipääsu krüpteerimiseks ja dekrüpteerimiseks vajalikele võtmetele. Kuna liidese kaudu on võimalik rollide lisamine, on võtmete turvalisus (näiteks nende hoidmine vastavas riistvaralises moodulis) oluline ning vajab riskipõhist ja lahendust haldava organisatsiooni olemasoleva taristuga sobilikku otsust.

Võtmehalduse protsess peab tagama, et OAuth liidesel on alati ligipääs tema teenuste pakkumiseks piisavalt turvalisele krüptograafilisele materjalile.

6.2.12 Standardite haldus

Lahenduse koosvõimeliseks toimimiseks olulised standardid vajavad pidevat hooldust ja tuge. Selle pakkumisega tegeleb standardite halduse protsess, mille eesmärgiks on tagada, et:

- kasutatavad standardid on igal ajahetkel kooskõlas tootekeskkonnas toimiva tarkvaraga;
- kasutatavad standardid oleksid kõigile osapooltele vabalt kätte- ja arusaadavad;
- osapooled oleksid standardite muutustest teadlikud reageerimiseks piisava viiteajaga;
- standardi versioonide muutus tootekeskkonnas toimuks tõrgeteta;
- standardid oleksid oma kirjelduses täpsed ja üheselt mõistetavad;
- osapooltel oleks võimalus standardite loomises ja arendamises süsteemselt kaasa rääkida.

6.2.13 Sõltuvuste haldus

Kesksel pääsuhalduse lahenduse keerukusel on kolm selgelt üksteisest eristuvat allikat:

- Algoritmiline keerukus, mis tuleneb keerukast arvutatavate rollide ning loogikast ning lahenduse funktsionaalsest konfigureeritavusest;
- Tehniline keerukus, mis tuleneb kõrgetest käideldavus- ja turvanõuetest;

[49] Vt p 6.1.2.5 ja 6.1.2.6.

- Kasutajakogemuse keerukus, mis tuleneb vajadusest toetada suurel määral kõikuvate vajadustega kasutajate rühmi.

Kõik kolm keerukuse komponenti on eraldiseisvalt hallatavad valmis teekide ja lahenduste kasutamisega. See tähendab aga, et keskne pääsuhalduse lahendus saab realiseerituna sõltuma suurest hulgast erisugustest erinevate tarnekadentsidega välistest komponentidest. Seetõttu on eriti oluline, et nii lahenduse tehnilise disaini kui käitamise faasides pööratakse tähelepanu kasutatavate teekide ajakohasusele ning suudetaks ennetada olukordi, kus teekide uuendamine näiteks turvanõuete tõttu ei ole võimalik ilma suuremahulise arendustööta.[50]

Seetõttu on lahenduse pideva toimimise aluseks sõltuvuste haldus, mis:

- Perioodiliselt valideerib kõigi lahenduse komponentide võimet kasutada kasutatavate teekide ja komponentide uusimaid kättesaadavaid versioone;
- Hindab vajadust teekide ja komponentide versioonide uuendamiseks;
- Annab sisendit arendusprotsessi juhtudel, kui teekide või komponentide uuendamiseks on vaja läbi viia arendustöid.

6.3 Infrastruktuur

6.3.1 Üldist

Pääsuhalduse lahendus kui tervik on loodud olema agnostiline infrastruktuuri suhtes - oleks keeruline luua süsteemi, mis seaks piiranguid klientsüsteemide ja allikregistrite kasutatavale infrastruktuurile minnes seega vastuollu x-tee ja riigi infosüsteemi arhitektuuri põhimõtetega.

Küll aga suhestub infrastruktuuriga olulisel moel keskne pääsuhalduse lahendus ning seega käsitletakse järgnevas just selle vastavaid vajadusi ning eeldusi. Siiski ei kirjeldata järgnevas konkreetseid tehnoloogilisi lahendusi: nii keerulise ja ebastandardse nõuete komplektiga süsteemi puhul on kriitiline, et nii süsteemi arendajad, hooldajad kui selle infrastruktuuri käitajad oleksid konkreetse tehnoloogilise lahendusega tuttavad ning et see sobituks olemasolevatesse tugi- ja arendusprotsessidesse. Seega tuleb tehnoloogilised otsused teha süsteemi disaini faasis kaasates kõiki olulisi osapooli, sealhulgas infoturbe eest vastutavaid rolle.

[50] Eriti tõsine probleem moodsate kasutajakogemuse raamistike puhul.

6.3.2 Pilvetaristu

Keskse pääsuhalduse lahenduse arhitektuur on loodud nii, et realiseeritud süsteem oleks suuteline vastama kehtestatud mittefunktsionaalsetele nõuetele, seda eriti käideldavuse ning vasteaja osas. Nii käideldavuse kui vasteaja tagamiseks peab teenuseid pakkuma rohkem kui ühe võimalikult spetsialiseeritud komponendiinstantsi abil, samuti peavad kõik andmehoidlad olema tükeldatavad. Seega on pääsuhalduse lahenduse komponentstruktuur loodud eeldama tüüpilise PaaS lahenduse võimalusi ning tema paigaldamine "puhta raua" kontekstis on pigem probleemne (kuigi kahtlemata võimalik).

Seejuures ei sõltu arhitektuur konkreetse PaaS platvormi realisatsioonist eeldades vaid võimet komponentide instantse sujuvalt lisada ja eemaldada ning ressursse vajadusel ümber jagada. Järelikult on pääsuhalduse keskne lahendus olemuslikult paigaldatav eri teenusepakkujate privaat- ja avalikes pilvedesse eeldusel, et disaini ja realisatsiooni faasis on tehtud vastavad otsused. Ehk, lahenduse arhitektuur ei sea piiranguid avaliku pilve kasutamisele. Küll aga võivad piirangud tuleneda lahendusele määratud E-ITS kaitsetarbe tasemest ning sellega seotud regulatsioonist.

On oluline mõista, et kasutataval infrastruktuurilahendusel on järelmid süsteemi käitamisel toimivatele protsessidele. Näiteks, kui kasutatakse virtuaalmasinate asemel konteineri põhist lahendust[51], liigub administratiivne vastutus paigaldatavat komponenti ümbritseva tarkvara ja selle konfiguratsiooni osas haldajalt arendajale. Konkreetse süsteemi kontekstis tähendab see tõenäoliselt vastutuse liikumist arenduspartnerilt RIA-le, mis kindlasti peab olema tagatud vastavate organisatoorsete meetmetega.

6.3.3 Võrk

Keskne pääsuhalduse lahendus ei tee rangeid eeldusi kasutatava võrguarhitektuuri osas. Küll aga on infoturbe perspektiivist mõistlik jagada lahenduse kasutatav võrgutaristu loogiliselt või krüptograafiliselt vähemalt järgmisteks selgelt eraldatud ning eraldi juhitud (ning turvatud) segmentideks:

- Liideste segment, kus asuvad komponendid, mis kas pakuvad või tarbivad väliseid teenuseid ning ka kasutajaliidese rakendus ning sellega kaasnevad teenused;
- Tundlike andmete segment, kus asuvad komponendid, mis käitlevad kas tundlikke või tervikluse mõttes olulisi andmeid;

[51] Esimesel juhul pakub pilvetaristu virtuaalset serverit, mille haldamine toimub tavaliselt virtuaalserveri eest tasuva organisatsiooni poolt. Teisel juhul pakub pilvetaristu sisuliselt võimalust käivitada kogu komponent koos teda ümbritseva tarkvaraga ühe läbipaistmatu ja arendaja kontrolli all oleva ühikuna.

- X-tee segment, kus asuvad lahendust teenindavad x-tee turvaserverid.

Selline jaotus võimaldab näiteks Konfiguratsioonihalduri ja Konfiguratsiooniadapteri paigaldamist eraldi võrgusegmentidesse võimaldades rakendada tundlikke andmeid sisaldavate komponentide suhtes oluliselt rangemaid turbepoliitikaid kui need kehtivad teenust pakkuvate komponentide suhtes.

Võrgu turbe mudelite osas võib rakendada nii permieetri kui kanali kontrolli, seejuures tuleb tagada, et Muutmisadapter ja Konfiguratsiooniadapter võiksid teenuse funktsionaalsuse kontrolli eesmärgil usaldada x-tee turvaserverist nendeni jõudnud päringute metaandmeid.

6.3.4 Hoidlad

Keskne pääsuhalduse lahendus sisaldab vähemalt järgmisi mahukaid kestvaid hoidlaid:

- Rollihalduri komponent:
  - Rollipuhver, kus hoitakse allikregistrite kohalikke koopiaid;
  - Rollide hoidla, kus hoitakse süsteemi enese poolt kontrollitavaid ja kas Kasutajaliidese või Muutmisadapteri kaudu muudetavaid rolle.
- Dokumendihalduri komponent:
  - Dokumendihoidla, kus hoitakse rolli määraja tahet väljendavaid elektrooniliselt allkirjastatud dokumente või vastavaid x-tee tõendeid.

Dokumendihaldur sisaldab lisaks äriloogikale ka võimekust säilitada potentsiaalselt suurt hulka potentsiaalselt suuri faile. Sellise võimekuse loomiseks on kõige praktilisem lahendus mõni S3-ühilduv objektihoidla, näiteks Ceph.

Rollihoidlaid iseloomustavad järgmised omadused:

- Nad ei sisalda muid andme-elemente peale seoste ning seega pigem ei sobi lahendamiseks traditsiooniliste relatsioonilise andmebaasi abil. Sobivam on kas graafi- või kolmikubaas. Eeldades, et süsteemi toetajad juba opereerivad relatsioonilisi andmebaase, võib osutuda mõistlikuks kasutada mõni relatsioonilisi andmebaase kestusmäluna kasutavat lahendust. Kuigi mitmed kolmikubaasid on mõeldud toetama semantilise veebi lahendusi ja arvutatavate rollide funktsionaalsus võib võita nende keerulisemast päringuloogikast, ei ole pääsuhalduse lahenduse toimimiseks täielik ressursikirjelduskarkassi ehk RDF-i tugi vajalik;

- Nende koormusprofiil on tugevalt kaldu lugemisele, rolli leidmine on oluliselt ajakriitilisem, kõrgemate tõrkenõuetega ning sagedasem toiming, kui rolli loomine. Seetõttu võib osutuda vajalikuks üks-mitmele kirjutamis- ja lugejakoopiate arhitektuur, kus üks kirjutatav andmebaasi instants replitseeritakse mitmeks loetavaks instantsiks;
- Nad on klasterdatavad nimeruumide kaupa. Samas toimuvad päringud mõlema seose otspunkti järgi ning seega on olulised kas indekseeritus või sekundaarne klasterdamine nii A kui B olemite järgi;
- Nende terviklus peab olema tagatud;[52]
- Ei eksisteeri rangeid nõudeid muutuste latentsi osas (st. ei ole sätestatud nõudeid selle kohta, kui kiiresti peab kirjutamisoperatsioon mõjutama lugemisoperatsioonide tulemust), kuid süsteem peab suutma garanteerida fikseeritud latentsi osana teenuslepingust.

Väiksemate koormusnõuetega ning seetõttu tehnilise realisatsiooni osas vabamate nõuetega hoidlaid sisaldavad veel järgmised komponendid:

- **Kasutajahaldur**, kes hoiab infot selle kohta, mis identiteedid on olnud huvitatud millistes kanalites milliste sõnumite saamisest;
- **Soovituste haldur**, kes hoiab seoseid rollide hulkade vahel.

Kõik mainitud hoidlad sisaldavad tundlikke isikuandmeid. On oluline mõista, et hoidlates töödeldavate isiku- ja muude andmete koosseis võib ajas muutuda, kui konfiguratsiooni lisatakse uusi allikregistreid ning kas luuakse või konfigureeritakse vastavad liidesed.

6.3.5 X-tee

Keskne pääsuhalduse lahendus suhtleb teiste süsteemidega peamiselt x-tee vahendusel. Seetõttu on x-tee turvaserverite kõrge käideldavus lahenduse toimimiseks oluline. Käideldavusnõuete tagamiseks on lahendusel x-tee turvaserverite osas järgmised nõuded:

- Turvaserverid peavad olema klasterdatud, kõiki teenuseid peab pakkuma vähemalt kaks turvaserveri instantsi;
- Teenuste pakkumiseks ja tarbimiseks kasutatavad turvaserverid peavad olema eraldatud tagamaks, et lahenduse võime teenuseid pakkuda ei sõltuks väliste osapoolte teenuse pakkumise võimekusest.[53]

[52] Vt p 3.
[53] Tarbitava teenuse madal läbilaskevõime võib põhjustada vastust ootavate päringute kuhjumise turvaserveris mis omakorda võib kahandada turvaserveri võimekust päringutele vastamisel

6.3.6 Logimine

Keskse pääsuhalduse lahenduse kaks peamist määratlevat nõuet on käideldavus ja turvalisus. Neist mõlemad eeldavad, et eksisteerib teadmine süsteemi olekust.

Tekitamaks teadmist süsteemi olekust, peab olema täidetud kaks tingimust:

- süsteemi moodustavad komponendid logima informatsiooni oma oleku kohta;
- eksisteerib võimekus loodud logide koondamiseks ning teadmuseks muutmiseks.

Neist esimene sõltub keskse pääsuhalduse lahenduse realisatsioonist, mille kõik komponendid peavad logima kõik olulised sündmused. Seejuures peavad logikirjed olema kas struktureeritud või stabiilse grammatikaga (st. struktureeritavad) ning sisaldama kirjega seotud päringu identifikaatorit.[54]

Neist teine toetub esimesele ning sõltub infrastruktuuri poolt pakutavast tarkvaralisest võimekusest koguda eri komponentide poolt toodetud logid ning teha need keskselt kättesaadavaks. Andmete kogumine loob omakorda eelduseks nende muutmiseks teadmuseks, ka see on infrastruktuuri poolt pakutava logilahenduse ülesanne, mis peab suutma pakkuda monitooringu, infoturbe ja andmekaitse protsesside nõuetele vastavat analüütikat. Need protsessid määravad ka logide säilituspoliitika ning, läbi tarkvara arenduse protsessi, suunavad üksikute sündmuste jõudmist logidesse.

Keskse pääsuhalduse lahenduse logid sisaldavad suure tõenäosusega tundlikke isikuandmeid või on muudetavad tundlikeks isikuandmeteks. Arendajale suunatud keeld mitte isikuandmeid logida ei saa olla efektiivne, sest ühe komponendi arendaja ei saa olla teadlik kogu süsteemi logide analüüsil tekkida võivast teadmusest. Seetõttu tuleb keskse pääsuhalduse lahenduse logisid käsitleda kui tundlikke isikuandmeid. Järelikult on andmekaitse protsessi ülesanne ühest küljest anda sisendit logide käitlemise lahendusse kuid teisalt ka dokumenteerida kehtivad logipoliitikat.

[54] Vt p 6.1.

7. Juhendmaterjalid

7.1 Integratsioonimustrid

7.1.1 Üldist

Käesolevas dokumendis kirjeldatud süsteem on keeruline, eeldab paljude osapoolte koostööd ning on disainitud võimalikult paindlikuks võimaldamaks suurt hulka eri viise temaga suhestumiseks. Järgnevas kirjeldatakse nelja peamist integratsioonimudelit. Neid on kindlasti võimalik omavahel kombineerida, all toodu on mõeldud mitte normatiivse vaid kirjeldavana.

Kõik mustrid eeldavad, et klientsüsteem on liitunud x-tee-ga.

Kõiki mustreid kirjeldatakse lihtsama võrdluse huvides neljas dimensioonis

- **Mudel on kasulik, kui**. Millistes olukordades on mudel kasulik?
- **Mudeli head küljed**. Miks just seda mudelit peaks kasutama?
- **Mudeli nõrgad küljed**. Miks mudelit ei peaks kasutama?
- **Mudeli kasutamiseks vajalikud eeldused**. Mida on mudeli rakendamiseks vaja teha?
- **Kasutajakogemus**. Kuidas mudel realiseerituna toimib ning kuidas lõppkasutajale välja paistab

Kõigi võimalike võimaluste hulgas pääsuhalduse lahendusega integreeruda võib eristada nelja peamist. Sõltuvalt asjaoludest võib kasutada ka nende kombinatsioone, asutuse eri süsteemid võivad kasutada eri mustreid ja võimalik on ka näiteks asutusesisese pääsuhalduse lahenduse integratsioon üle-riikliku lahendusega. Neli peamist integratsioonimustrit on:

- **Minimaalne integratsioon**, kus klientsüsteemi õigused on keskselt nähtavad kuid mitte muudetavad
- **Osaline integratsioon**, kus klientsüsteemi õigused on keskselt nii nähtavad kui muudetavad
- **Täisintegratsioon**, kus klientsüsteem ei oma üldse pääsuhalduse lahendust
- **Alliksüsteemi integratsioon**, kus klientsüsteem kasutab küll pääsuhalduse lahenduse standardeid kuid suhtleb otse ühe või rohkema allikregistriga

7.1.2 Minimaalne integratsioon

- Mudel on kasulik, kui

    - Klientsüsteemi olulisem muutmine ei ole võimalik või otstarbekas ning samuti ei ole võimalik või otstarbekas klientsüsteemi käideldavuse või äriprotsesside muutmine nii, et süsteem oleks võimeline vastu võtma keskse pääsuhalduse lahenduse poolseid päringuid rollide lisamiseks ja muutmiseks;
    - Eesmärgiks on kiire integratsioon teel näiteks osalise integratsiooni poole või valideerimaks integratsiooni võimalikkust;
    - Klientsüsteemil eksisteerib hulk keerulisi erivajadusi, mis välistavad rollide lisamise ja eemaldamise kolmandate osapoolte poolt.[55]
- Mudeli hea külg:
    - Võimaldab klientsüsteemil minimaalsete kuludega saavutada kasulik kasutajakogemus, kus kasutaja näeb keskset ülevaadet kõigist oma rollidest.
- Mudeli nõrk külg:
    - Kasutaja peab pendeldama eri süsteemide vahel.
- Mudeli kasutamiseks vajalikud eeldused:
    - Klientsüsteemi ja keskse pääsuhalduse lahenduse vahel on läbi viidud kõik formaalsused, mis on vajalikud keskse pääsuhalduse lahenduse ligipääsuks pakutavate x-tee teenustele;
    - Klientsüsteem on realiseerinud tarkvara, mis suudab vastata keskse pääsuhalduslahenduse päringutele õiguste kohta;
    - Keskselt on kirjeldatud kõik rollid, mida klientsüsteem pakub. Nende alliksüsteemiks on määratud klientsüsteem. Kõik rollid on märgitud kliendi poolt mitte muudetavaks koos viitega klientsüsteemi vastavasse protsessivoogu.
- Kasutajakogemus:
    - Klient logib klientsüsteemi teenusesse ja saab seal õigusi määrata, neid vaadata ning sooritada mis iganes toiminguid õigused tal võimaldavad teha. Klientsüsteem võib selleks kõigeks kasutada milliseid iganes väliseid allikaid;
    - Klient võib sisse logida kesksesse pääsuhalduslahendusse ning seal näha nii seda, mis rollid on talle konkreetses klientsüsteemis antud kui ka seda, mis õigused ta on andnud kas enda või oma esindatavate nimel. Ta saab vajutada linki, mis viib ta klientsüsteemi rollide haldamise äriprotsessi.

[55] Vastupidine protsess, kus keeruline pääsuhalduste loogika peegeldatakse rollideks on alati võimalik: iga õigus toiminguks on väljendatav seosena.

7.1.3 Osaline integratsioon

- Mudel on kasulik, kui:
    - Klientsüsteemil on spetsiifilised vajadused pääsuõiguste halduse suhtes, kuid on võimekus luua seos rollipõhise pääsuhaldusega nii rollide lugemiseks kui kirjutamiseks keskse lahenduse poolt;
    - Klientsüsteemil on oluline vajadus säilitada täielik kontroll oma äriprotsessi ja toimepidevuse üle.
- Mudeli hea külg:
    - Võimaldab klientsüsteemil säilitada täielik kontroll oma äriprotsessi ja toimepidevuse üle.
- Mudeli nõrgad küljed:
    - Tehniliselt suhteliselt keeruline protsess;
    - Klientsüsteemil ei kao vajadus teha kulutusi oma äriprotsessi ja selle realisatsiooni osas kuid keskele tuleb kulutusi juurde.
- Mudeli kasutamiseks vajalikud eeldused:
    - Klientsüsteemi ja keskse pääsuhalduse lahenduse vahel on läbi viidud kõik formaalsused, mis on vajalikud keskse pääsuhalduse lahenduse ligipääsuks pakutavate x-tee teenustele;
    - Klientsüsteem on realiseerinud tarkvara, mis suudab vastata keskse pääsuhalduslahenduse päringutele õiguste kohta ning päringutele, mis rolle lisavad ja eemaldavad;
    - Keskselt on kirjeldatud kõik rollid, mida klientsüsteem pakub. Nende alliksüsteemiks on määratud klientsüsteem.
- Kasutajakogemus:
    - Klient logib klientsüsteemi teenusesse ja saab seal õigusi määrata, neid vaadata ning sooritada mis iganes toiminguid õigused tal võimaldavad teha. Klientsüsteem võib selleks kõigeks kasutada milliseid iganes väliseid allikaid;
    - Klient võib sisse logida kesksesse pääsuhalduslahendusse ning seal näha nii seda, mis õigused on talle konkreetses klientsüsteemis antud kui ka seda, mis õigused ta on andnud kas enda või oma esindatavate nimel. Ta saab õigusi lisada ja eemaldada, kõik muutused sooritatakse liideste vahendusel alliksüsteemis.[56]

[56] Invalideerides kohaliku vahemälu

7.1.4 Täisintegratsioon

- Mudel on kasulik, kui:
    - klientsüsteem on kas alles arendamisel või on läbimas olulisi muutusi, sel juhul on klientsüsteemi enese pääsuhalduse lahendusest loobumine või selle süsteemist eemaldamine kõige põhjalikum ja valutum;
    - klientsüsteemil ei ole pääsuhalduse suhtes erivajadusi (laialdane atribuudi- või nimekirjapõhine pääsuhaldus, ülimalt kõrged käideldavusnõuded vms.) või õigustavad madalad arendus- ja halduskulud nendest loobumist;
    - klientsüsteemi vajadused pääsuhalduse suhtes on minimaalsed piirdudes mõne rolliga või vajades näiteks ainult juriidilise esindaja või eestkostja rolli.
- Mudeli hea külg:
    - Mudeli kasutamine võimaldab klientsüsteemil loobuda kõigist pääsuhaldusega seotud äriprotsessidest ja nende tehnilisest realisatsioonist.
- Mudeli nõrk külg:
    - Tekitab kriitilise sõltuvuse kesksest pääsuhalduse süsteemist nii funktsionaalsuse kui käideldavuse mõttes.
- Mudeli kasutamiseks vajalikud eeldused:
    - Klientsüsteemi ja keskse pääsuhalduse lahenduse vahel on läbi viidud kõik formaalsused, mis on vajalikud klientsüsteemi ligipääsuks pakutavate x-tee teenustele;
    - Klientsüsteem on realiseerinud tarkvara, mis suudab osana teenusest esitada korrektseid päringuid keskselе pääsuhalduse lahendusele;
    - Klientsüsteemi haldav organisatsioon on realiseerinud tehnilised ja organisatoorsed meetmed x-tee tõrgete, sidehäirete ja keskse pääsuhalduse lahenduse toimepidevuse häiretega toime tulekuks;
    - Kõik vajalikud rollid on keskselt kirjeldatud ja/või mõnest allikregistrist otse kättesaadavad.
- Kasutajakogemus:
    - Klient logib klientsüsteemi sisse;
    - Klientsüsteem võib esitada päringu "*:B:X" leidmaks kõiki osapooli, keda kodanik esindab. Päring esitatakse kõigi rollide X kohta, millest tuleneb konkreetse teenuse protsessis esindusõigus;

- Klient läbib äriprotsessi, kuni jõuab operatsioonini, mis vajab konkreetse rolli olemasolu;
- Klientsüsteem esitab päringu "A:B:X" kontrollimaks, kas konkreetne roll on ka operatsiooni tegemise hetkel olemas;
- Klient võib sisse logida kesksesse pääsuhalduse lahendusse ning sooritada kõigi talle või tema esindatavatele määratud või tema või tema esindatavate poolt määratud kõiki konfiguratsiooni poolt lubatud toiminguid.

7.1.5 Alliksüsteemi integratsioon

- Mudel on kasulik, kui:
  - Klientsüsteemi vajadused piirduvad vaid otse allikregistritest tulenevate rollidega, näiteks esindus- või hooldusõigus
- Mudeli head küljed:
  - Võimaldab klientsüsteemil kasutada minimaalset vajalikku funktsionaalsust (kasutaja õigus esindada juriidilist isikut, näiteks) tekitamata sõltuvust kesksest lahendusest;
  - Võimaldab klientsüsteemil sujuvalt üle minna keskse pääsuhalduslahenduse kasutamisele, kui rollid ja vajadus keerukamaks muutuvad.
- Mudeli nõrk külg:
  - Eeldab, et allikregistrid on realiseerinud oraakliliidese, mida süsteemi kui terviku toimimiseks tingimata vaja ei ole.
- Mudeli kasutamiseks vajalikud eeldused:
  - Klientsüsteemi ja allikregistrite vahel on läbi viidud kõik formaalsused, mis on vajalikud keskse pääsuhalduse lahenduse ligipääsuks pakutavate x-tee teenustele;
  - Klientsüsteem on realiseerinud tarkvara, mis suudab osana teenusest esitada korrektseid päringuid allikregistritele;
  - Alliksüsteemi poolt pakutavad rollid on keskselt kirjeldatud.
- Kasutajakogemus:
  - Klient logib klientsüsteemi sisse;
  - Klientsüsteem võib esitada allikregistrile või -registritele päringu "*:B:X" leidmaks kõiki osapooli, keda klient esindab. Päring esitatakse kõigi rollide X kohta, millest tuleneb konkreetse teenuse protsessis esindusõigus;

- Klient läbib äriprotsessi, kuni jõuab operatsioonini, mis vajab konkreetse õiguse olemasolu;
- Klientsüsteem esitab allikregistrile päringu "A:B:X" kontrollimaks, kas konkreetne õigus on olemas. See on oluline igal juhul teha, sest õigus võib olla vahepeal kadunud;
- Klient võib sisse logida kesksesse pääsuhalduse lahendusse ning sooritada kõigi talle või tema esindatavatele määratud või tema või tema esindatavate poolt määratud kõiki konfiguratsiooni poolt lubatud toiminguid.

7.2 Pääsuhalduse juhtumid ja nende lahendamine

7.2.1 Üldist

All-toodud näited ei ole normatiivsed ning kirjeldavad vaid ühte paljudest võimalustest juhtumite lahendamiseks. Näidete nimekiri on kogutud intervjuude ja käesoleva dokumendi tagasiside protsessi käigus ning ei ole lõplik (st. ei määratle lõplikult kogu lahenduse pakutavat funktsionaalsust).

Juhtumid, mis vajavad arvutatavate rollide funktsionaalsust, eeldavad, et realiseeritud on UC20.

7.2.2 Eesti Energia töötajate juhtum

Olgu meil suur ja paljude töötajate ning keerulise kontsernistruktuuriga organisatsioon, näiteks Eesti Energia või Tallinna linnavalitsus. Ühest küljest on sellisel organisatsioonil kindlasti vajadus hallata neid esindavate isikute õigusi kuid teisalt on selliseid isikuid tõenäoliselt palju ning tõenäoliselt on vastavad protsessid ka elektroonilised või isegi automatiseeritud. Seetõttu ei oleks mõistlik pakkuda sellistele organisatsioonidele vaid käsitsi õiguste lisamise ja eemaldamise funktsionaalsust.

Antud kaasuse lahendamiseks käesolevas dokumendis kirjeldatud süsteemi abil on kaks põhimõttelist võimalust.

1) Organisatsioon lisab ja eemaldab neile vajalikud muutused neid esindavate organisatsioonide rollides kasutades masinliideseid. Kuna ka keskne pääsuhalduse süsteem ise saab klientsüsteemides rolle lisada ja eemaldada, on vastavad liidesed standardiseeritud. Keskne pääsuhalduse süsteem peab seejuures kontrollima, et x-tee

kaudu lisatavad ja eemaldatavad õigused oleksid ainult selle organisatsiooni omad, kelle x-tee turvaserverist vastavad päringud saabuvad;

2) Organisatsioon muutub sisuliselt allikregistriks ning "Eesti Energia töötaja" (või mis iganes muu organisatsiooni töötaja) roll saab keskses konfiguratsioonis kirjeldatud. Liidestatav organisatsioon peab oma sisemise pääsuhalduse süsteemi teistele osapooltele kättesaadavaks tegema[57] ning edaspidi on nii neil, kui kõigil teistel osapooltel võimalik kontrollida, kas konkreetsel isikul on vastav roll. Samuti on võimalik luua arvutatavaid rolle, kus konkreetse asutuse töötaja rollist tuleneb mõni üldisem, näiteks raamatupidaja või aruande esitaja roll. Nii ei pea osapooled teadma midagi konkreetse asutuse liidestustest ning võivad edasi kasutada oma äriprotsessi kontekstis selget kasutajaõiguste semantikat.

Neist esimene võimalus on selgesti eelistatum, kuna eraldab selgemini organisatsiooni ja üleriikliku pääsuhalduse äriprotsessid. Samuti on nii toimides madalamad nõuded organisatsiooni enese infosüsteemide käideldavusele. Teine võimalus, samas, võimaldab realiseerida erindeid, kus näiteks konkreetse organisatsiooni vajadustest lähtudes on mitmel osapoolel vaja muuta rollide semantikat. Näiteks võib eksisteerida ainult suurtele ettevõtetele mõeldud "raamatupidaja abi" roll, millele rakendub eraldi õiguste komplekt.

7.2.3 KOV-i ametnike juhtum

Olgu meil vaja luua võimalus kontrollida, kas konkreetne isik on mõne kohaliku omavalitsuse ametnik. Kirjeldatava süsteemi mõttes on tegemist seosega era- ja juriidilise isiku vahel. Põhjus sellise rolli lisamiseks võib olla näiteks vajadus kontrollida ametniku õigust sooritada mingeid toiminguid (näiteks elukaarega seotud sündmusteenuste, MTA teenuste vms. raames) või realiseerida keerukamat äriprotsessi[58], kus näiteks käsitletakse olukorda, kus isiku hooldusõigus on üle läinud KOV-ile.

Kindlasti on kirjeldatud vajadus võimalik realiseerida kirjeldades vastavad rollid ning lähtudes eelpool kirjeldatud suure organisatsiooni mallist.[59] Kuid on ka teine võimalus. Selle realiseerimiseks peab olema täidetud kaks eeldust:

1) Peab eksisteerima allikas (näiteks äriregister), mis on suuteline pidama ja jagama KOV-ide nimekirja väljastades seost "KOV" Eesti Vabariigi ja konkreetse juriidilise isiku vahel. Nii on võimalik kontrollida, et esindatav isik ka tõesti KOV on;

[57] Vähemalt minimaalse integratsiooni tasemel, vt p 7.1.2.
[58] Näiteks, kuid mitte tingimata, arvutatavate rollide kaudu
[59] Vt p 7.2.2

2) Peab eksisteerima allikas (näiteks RTK), kes on suuteline väljastama seost "ametnik" juriidilise isiku ja eraisiku vahel.

Nende eelduste täidetusel saab näiteks defineerida arvutatava rolli "esindusõigus", mis on seos eraisikute vahel ning mis saadakse lihtsalt leides esindatav.juriidiline_hooldaja.ametnik. Samuti on kõigil osapooltel võimalik alati kontrollida, kas ja milliste juriidiliste isikute suhtes on sisse loginud kasutajal roll "ametnik".

7.2.4 Paljude rollide juhtum

Olgu meil vaja piirata ligipääsu teenusele sõltuvalt kasutaja rollist. Näiteks võib teenuses olla võimalik teha toiminguid ametnikuna, juriidilise isiku esindajana või eraisikuna. Igaühel neist võivad olla õigused eri toiminguteks, seejuures ametniku ja juriidilise isiku esindajana ka sama juriidilise isiku suhtes. Samuti võivad kasutajal olla eri juriidiliste isikute suhtes erinevad õigused.

Selline olukord on lahendatav ainult teenusrakenduse aktiivse koostöö abil. Keskne pääsuhalduse lahendus ei tea, kes ja mis autentimisvahendiga on sisse loginud, millist rakenduse osa parasjagu kasutatakse või milliseid valikuid ollakse teinud. Seega ei tea pääsuhalduse süsteem midagi kasutaja hetkel aktiivsest rollist ning ei saa seega ka vastata küsimusele "mida tohib kasutaja A ametnikuna teha juriidilise isiku B suhtes".[60]

Vajalik funktsionaalsus saadakse kasutades ka praegu sagedasti realiseeritud malli, kus esmalt tehakse kindlaks esindatavad isikud ning seejärel võimaldatakse kasutajal nende vahel valida. Samuti võib rakenduse poolt pakutav kasutajakogemus (lisaks lubatud toimingute komplektile) kohanduda parasjagu valitud rollile.

Pärast kasutaja autentimist teeb klientsüsteem päringu leidmaks kasutaja poolt esindatavad isikud. Milliseid rolle seejuures kontrollitakse, on klientsüsteemi äriloogika osa. Tehniliselt käivitatakse iga rakendusele huvi pakkuva rolli kohta kas keskse pääsuhalduse süsteemi oraakliliidese või otse mõni allikregistri suunas päring *:B:X, kus B on parasjagu sisse loginud kasutaja identifikaator ning X otsitav roll. Näiteks võib päringu *:isikukood:juhatuse_liige suunata nii äriregistri[61] kui keskse pääsuhalduse suunas. Saadud tulemuste ühendist moodustubki sisse loginud kasutaja poolt esindatavate isikute nimekiri.

[60] Põhimõtteliselt on võimalik realiseerida keskne persoonade süsteem, kus ühel identiteedil võib olla mitu erinevate õigustega persoonat. Siiski lisaks selline lahendus oluliselt keerukust keskses süsteemi (seda nii tehnilise lahenduse kui kasutajaliidese osas) ning ei vähendaks oluliselt klientsüsteemide keerukust.
[61] Eeldusel, et äriregister allikregistrina on realiseerinud vastava liidese

Saadud isikute nimekirjast võib kasutaja valida, keda ta mingis rollis esindab, ning rakendus seepeale kas lubab või keelab vastavad toimingud. Toimingu sooritamisel tuleb igal juhul kontrollida selleks vajaliku rolli olemasolu. Ühest küljest võivad rollid muutuda kuid teisalt ei pea esindamiseks vajalik roll olema piisav kõigi toimingute sooritamiseks kuid teisalt tuleb enne toimingu tegemist veenduda ka selles, et kasutajal pole õnnestunud selleks mitte ette nähtud viisil konteksti vahetada.

7.2.5 Kliendihalduri juhtum

Olgu meil vaja kontrollida, kas kasutaja on konkreetse kliendi kliendihaldur või ei. Üldiselt ei ole sedalaadi probleeme mõistlik lahendada käesolevas dokumendis kirjeldatud pääsuhalduse lahenduse abil, sest enamasti on kliendi ja kliendihalduri suhe ühe organisatsiooni sisene. Ehk, teistel asutustel puudub vajadus või isegi õigus teada, kes konkreetse kliendiga tegeleb ning seega ei ole ka mõistlik ei tehnilist ega funktsionaalset lahendust muuta keerulisemaks, kui hädasti vajalik. Keskse pääsuhalduse kasutamine siinkohal on seega õigustatud ainult juhul, kui kliendi ja kliendihalduri vahelist seost on vaja jagada mitmete osapoolte vahel. Ka sellisel juhul tuleb arvestada, et kliendihalduri roll on avalik kõigi pääsuhalduse süsteemiga liidestunud osapoolte vahel.

Kui on aga vajadus kliendihalduri probleem keskse pääsuhalduslahenduse abil lahendada, siis kirjeldatakse selleks roll "kliendihaldur", mis on seos era- ja juriidilise isiku vahel ja mille alliksüsteemiks on milline iganes süsteem, kus seda suhet kirjeldatakse.[62] Kui alliksüsteem on vastavad standardsed liidesed realiseerinud, on kõigil osapooltel võimalik kontrollida, kas kasutaja on konkreetse kliendi kliendihaldur või mitte.

7.2.6 Advokaadi ja advokaadibüroo juhtum

Olgu meil tarvis lahendada (hüpoteetiline) olukord, kus toimikule peavad pääsema ligi hulk eri advokaadibüroode töötajaid. Kuna advokaadibürood võivad eri juhtumites esindada mõlemaid osapooli on oluline, et oleks välistatud huvide konflikt mitte lubades toimikut lugeda isikutel, kes esindavad mõlemat osapoolt.

Tehniliselt võib käesoleva süsteemi raames kirjeldada soovi nii, et rollis "toimiku vaataja" on isikud, kellel on toimikuga seoses "hageja" oleva organisatsiooniga seoses "juriidiline

[62] Juhul, kui kliendihalduri roll on määratav kliendi enda poolt, on tegu tavalise rollide määramise juhtumiga. Alternatiivina võib seoseid klientide ja nende haldurite vahel lisada ka masinliidese abil

esindaja" oleva organisatsiooniga seos "advokaat" või "advokaadi abi" ja kes samal ei ole seoses "toimiku vaataja" organisatsiooni suhtes, kellel on toimikuga seos "kostja".

Sellise lahenduse realiseerimiseks tuleb defineerida järgmised rollid:

- "Advokaat", mis on seos era- ja juriidilise isiku vahel ja mida määrab juriidilise isiku esindaja;
- "Advokaadi abi", mis on seos eraisikute vahel ning mida määrab üks isikutest;
- "Kostja", mis on seos toimiku ja juriidilise isiku vahel ja mille alliksüsteemiks on RIK-i infosüsteem;
- "Hageja", mis on seos toimiku ja juriidilise isiku vahel ja mille alliksüsteemiks on RIK-i infosüsteem;
- "Esindaja", mis on seos juriidiliste isikute vahel;
- "Toimiku vaataja hageja poolelt", mis on arvutatud roll toimiku ja eraisiku vahel ja saadakse toimik.hageja.esindaja.advokaat + toimik.hageja.esindaja.advokaat.advokaadi_abi;
- "Toimiku vaataja kostja poolelt", mis on arvutatud roll toimiku ja eraisiku vahel ja saadakse toimik.kostja.esindaja.advokaat + toimik.kostja.esindaja.advokaat.advokaadi_abi;
- "Toimiku vaataja", mis on arvutatud roll toimiku ja eraisiku vahel ja saadakse (toimik.vaataja_hageja_poolelt - toimik.vaataja_kostja poolelt) + (toimik.vaataja_kostja_poolelt - toimik.vaataja_hageja poolelt).

Samuti tuleb kirjeldada toimiku identiteet ning realiseerida RIKi poolt liides toimiku identifikaatori lahendamiseks inimloetavaks nimeks.

Kirjeldatud konfiguratsioonimuudatuste järel peab RIK tegema kättesaadavaks liidesed väljastamaks seoseid toimikute, kostjate ja hagejate vahel ning advokaadibüroode esindajad peavad määrama isikud advokaadi rollidesse. Viimased võivad omakorda määrata isikuid advokaadi abi rollidesse.[63]

Seejärel on võimalik osapoolel, kes peab kontrollima ligipääsuõigusi toimikule kontrollida seose "toimiku vaataja" olemasolu konkreetse toimiku ning sisse loginud kasutaja vahel. Sellise päringu saanuna toimib keskne pääsuhalduse lahenduse nii:

- Leiab konfiguratsioonist rolli "toimiku vaataja" (tehniliselt optimeeritud) kirjelduse;

[63] Kuna advokaadi abi on määratud advokaadi poolt, tekib olukord, kus advokaadi abid on seotud advokaadi ja mitte bürooga. Ehk, kui advokaat bürood vahetab, säilitavad büroo töötajad tema suhtes advokaadi abi rollid

- Leiab, et vastuse saamiseks on vaja kontrollida isiku kuulumist hulkadesse toimik.vaataja_hageja_poolelt ning toimik.vaataja_kostja_poolelt;
- Leiab nende rollide (tehniliselt optimeeritud) kirjeldused;
- Leiab, et selleks peab ta kontrollima kasutaja kuulumist hulkadesse toimik.hageja.esindaja.advokaat, toimik.hageja.esindaja.advokaat.advokaadi_abi, toimik.kostja.esindaja.advokaat.advokaadi_abi ja toimik.kostja.advokaat.advokaadi_abi;
- Leiab kõik konkreetse toimikuga seotud hagejad ja kostjad;
- Leiab kõigi nendega seoses "esindaja" olevad isikud;
- Leiab kõigi leitud esindajatega seoses "advokaat" olevad isikud;
- Leiab kõigi leitud advokaatidega seoses "advokaadi_abi" olevad isikud;
- Sooritab konfiguratsioonis kirjeldatud hulgaoperatsioonid;
- Kontrollib, kas isik kuulub tehte tulemusena saadud hulka või mitte.

7.2.7 AAR-i juhtum

Olgu meil olukord, kus olemasolev kuid elutsükli lõpus asuv lahendus pakub osapooltele pääsuhaldusega seotud teenuseid. Ühest küljest on sel juhul eesmärgiks olemasoleva lahenduse võimalikult kiire sulgemine kuid teisalt tuleb minimeerida seda kasutavate osapoolte tehtavaid muutusi ning nende elutsüklit.

Sel juhul on üks võimalusi olukorra lahendamiseks olemasoleva süsteemi käsitlemine uue pääsuhalduse lahenduse kontekstis tavalise klientsüsteemina. Rakendatakse täisintegratsiooni mustrit[64] ning kõik vanas süsteemis eksisteerivad rollid muutuvad nii nähtavaks kui muudetavaks läbi uue pääsuhalduse lahenduse. Olemasoleva lahenduse lõppkasutajad võib suunata kas kohe või mõningase üleminekuajaga keskset pääsuhalduse lahendust tarvitama ning, kui viimased klientsüsteemid on kesksele lahendusele kolinud, võib vana lahenduse sulgeda.

7.2.8 Vahendatud x-tee päringu juhtum

Olgu meil olukord, kus mõne riigi infosüsteemi osaga soovib suhelda osapool, kellel puudub võimekus või soov opereerida oma infosüsteemi või seda riigi infosüsteemiga siduvaid x-tee turvaservereid. Oma äriliste vajaduste rahuldamiseks on ta astunud

[64] Võib rakendada ka minimaalse- või osalise integratsiooni mustrit, kuid sel juhul pikeneb periood, mil lõppkasutaja kohtub kahe erineva kasutajaliidesega.

lepingulisse suhtesse teenusepakkujaga, kes opereerib nii kliendi infosüsteemi kui ka vastavaid x-tee turvaservereid. Kuigi x-teel on võimalik eristada ja pääsuõiguste määramisel kasutada teenusepakkuja ja x-tee turvaserveri operaatori rolle, ei pruugi selline lähenemine antud juhul anda piisavat tulemust: kuna kliendil puudub igasugune kontroll talle teenust pakkuva taristu üle, ei pruugi ta omada ka piisavat kontrolli x-tee turvaserveri poolt kasutatava privaatvõtme üle.

Sellise stsenaariumi lahendamiseks pakub pääsuhalduse süsteem järgmist lahendust.

- Kirjeldatakse juriidilisi isikuid siduv roll "x-tee esindaja";
- Kliendi esindaja logib kesksesse pääsuhalduse lahendusse ning määrab teenusepakkuja seal kliendi suhtes rolli "x-tee esindaja";
- Iga riigi infosüsteemi osa, saades kliendi nimel[65] päringu teenusepakkujalt, võib pääsuhalduse lahendusele esitada päringu, kas kliendi ja teenusepakkuja vahel eksisteerib roll "x-tee esindaja";
- Kliendi esindaja võib igal hetkel logida sisse kesksesse pääsuhalduse lahendusse ning eemaldada kõik seosed klientorganisatsiooni ja teenusepakkuja vahel misjärel juba järgmine päring rolli olemasolu kontrolliva riigi infosüsteemi osa suunas ebaõnnestub. Samal tasemel kontrolli saavutamine x-tee kasutatava privaatvõtme üle eeldaks aga kindlasti toimivat koostööd teenusepakkujaga.

7.2.9 Notariaalsete volikirjade juhtum

Olgu meil olukord, kus asutus A aktsepteerib oma infosüsteemis õiguste lisamiseks või eemaldamiseks notariaalselt kinnitatud volikirja. Ehk, kodanik võib toimetada asutusse A notari poolt kinnitatud volikirja esindada organisatsiooni B , mille alusel lisatakse talle infosüsteemis vastavad õigused. Seejuures ei ole notariaalsed volikirjad koondatud ühtsesse masinloetavasse andmebaasi ning asutus A võib kuid ei pruugi[66] realiseerida äriprotsessi Ametlike Teadaannete kasutajaliidese[67] jälgimiseks, et tuvastada volikirja kehtetuks tunnistamine.

Pääsuhalduse lahenduse vaatepunktist on notariaalsetel volikirjadel kaks põhimõttelist puudust: volikiri on oma loomult vabavormiline ning need ei ole kättesaadavad

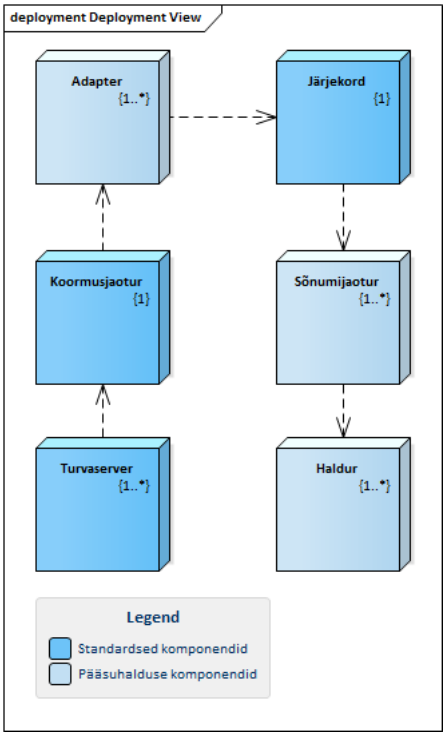
[65] Seejuures võib kliendi viide olla esitatud kas päringu parameetrites või läbi x-tee enese esindusmehhanismide.
[66] Osa küsitletud asutustest, kes notariaalseid volikirju aktsepteerivad, ei ole sellist äriprotsessi volikirjade ja nende kehtetuks tunnistamise sündmuse suhtelise vähesuse tõttu realiseerinud.
[67] Süsteemil puudub masinliides.

masinliidese kaudu. Ehk, isegi, kui notariaalsete volikirjade kohta eksisteeriks kättesaadav vastavate liidestega varustatud andmebaas, tuleks volikirja sisu siiski sisuliselt interpreteerida mõistmaks, mis rollideks ja kellega seoses konkreetne dokument aluse annab. Pääsuhalduse lahendus aga ei tegele rollide allikate ega nende kasutamise tõlgendamisega.[68]

Seega tuleb notariaalsete volikirjade pääsuhalduse lahenduse kaudu kättesaadavaks tegemiseks realiseerida protsess, mis volikirja sisust konkreetsed rollid järeldab ning infosüsteem, mis nii saadud rolle korrektselt interpreteerib. Asutusel A on mõlemad olemas. Järelikult on notariaalsete volikirjade puhul kõige mõistlikum olukord, kus klientsüsteem realiseerib nii vajalikud äriprotsessid ja loogika ning teeb tulemuse mõnda integratsioonimustrit kasutades teistele osapooltele kättesaadavaks.

7.3 Liideste skaleeruvuse näide

Infosüsteemide skaleeruvaks integratsiooniks on mitmesuguseid võimalusi. Juhtudel, kui oluline on kahesuunaline side (st. päringutele oodatakse ka vastuseid), on levinud päring-vastus muster.[69] Selle mustri puhul edastatakse päringud päringujärjekorda, mille teises otsas loetakse päringud, töödeldakse ning lisatakse vastused vastusjärjekorda. Sellise mustri peamiseks heaks omaduseks on, et kliendi dünaamiliselt keeruline käitumine ei pane keerukalt käituma serverit, ehk keskset pääsuhalduse lahendust. Samuti võimaldab muster sujuvalt koormust ringi jagada, viisakalt reageerida tõrgetele, prioritiseerida päringuid, efektiivselt mõõta süsteemi võimet koormusega toime tulla ning kasutada süsteemi ressursse võimalikult efektiivselt. Lihtsamates olukordades teenib sama eesmärki jagatud fikseeritud suurusega ühenduste hulga kasutamine



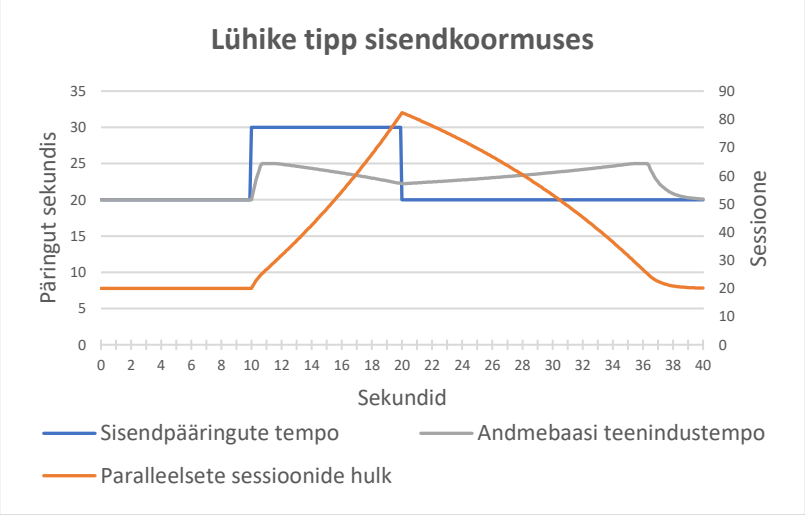
Joonis 6. Turvaserveri puhverdamine järjekorra abil

[68] Vt p 4.
[69] Ingl. *Request-Reply*. Hohpe, Gregor, and Bobby Woolf. *Enterprise integration patterns: Designing, building, and deploying messaging solutions*. Addison-Wesley Professional, 2004.

teenindavate süsteemide suhtlemiseks kuid paljude klientide ja serverite puhul ei ole see muster mõistlik.

Ühte võimalikku viisi punktis 5.2 kirjeldatud komponentide mustrit paigaldada kujutab Joonis 6. Sel juhul suunatakse turvaserverite klastri[70] päringud esmalt läbi koormusjaoturi olekuvabade adapterite klastrini. Seal rakendatakse päringule ärireeglid ning formuleeritakse päringud teenust reaalselt pakkuvate halduriteni. Päringud suunatakse järjekorda ning adapter jätab meelde seose välja läinud päringu ning vastust ootava võrguühenduse vahel. Päringut töödelnud lõim vabastatakse. Kuna lahenduse puhul on oluline kiire ja töökindel vastus ja mitte vastus igal juhul, võib järjekord olla olekuvaba ehk mittepüsiv. Järjekorra teises otsas loeb olekuvaba sõnumijaotur järjekorrast päringu ning otsustab, millisele halduri instantsile see töötlemiseks suunata. Seejärel suunatakse päring täitmisele ning sõnumijaotur jääb vastust ootama. Olles vastuse saanud, suunab ta selle vastusjärjekorda ning asub töötlema järgmist päringut. Adapter loeb vastusjärjekorrast vastuse saadetud päringule, leiab mälust seda ootava võrguühenduse viite ning saadab vastuse koormusjaoturi vahendusel ootavale turvaserverile. Süsteemi suure koormuse korral, kui adapter ei ole määratud aja jooksul vastust saanud, võib ta liiga kaua ootavatele võrguühendustele saata vastava veateate. Samuti võib liiga kaua vastust oodanud sõnumeid järjekorrast kõrvaldada järjekorrahaldur.

Joonis 6 näitab, et päring läbib enne töötlemist mitmeid komponente ning võib vastust oodata suhteliselt kaua. Seetõttu on mustri realiseerimise oluliseks eelduseks madal latents seadmete vahel. Pilvekeskkonnas, kus mitmed paigaldustipud võivad jagada sama riistvara ning kus võrguühendus on sageli virtualiseeritud, ei ole seadmete vaheline side reeglina takistuseks.

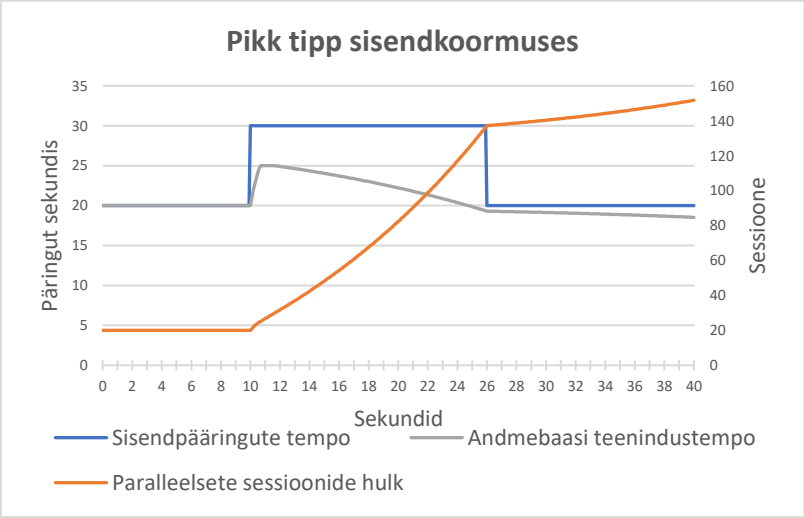


Joonis 7. Puhverdamata süsteemi käitumine lühikese sisendkoormuse tipu puhul

[70] Turvaserverite klasterdamise problemaatika on väljaspool käesoleva dokumendi ulatust, turvaservereid loetakse sisuliselt lõputult skaleeruvaks.

Kindlasti lisavad aga suur hulk eri komponente teatud määral töötlusaega ning vajab põhjendamist, miks kirjeldatud muster koormuse all paremini toimib, kui otseside adapteri ja halduri vahel.

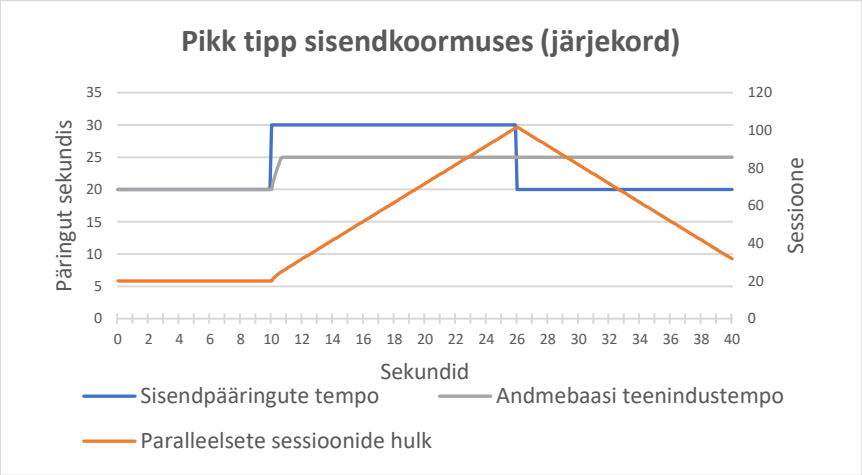
Vastuse annab mudeldamine. Kasutatud mudel koosneb päringuid genereerivast klientsüsteemist ning neid teenindavast andmebaasist. Eeldatud on, et sisendkoormuses toimub ajutine kuid oluline kasv. Samuti on tehtud realistlik eeldus, et paralleelsete päringute puhul nende töötlusaeg kasvab, kuna päringud hakkavad ootama jagatud piiratud ressursi vabanemist teenindavas serveris.[71] Selline mudel vastab reaalsusele, sest sisendkoormus tõe poolest kõigub ning kasvav paralleelselt teenindavate päringute hulk pikendab tõesti nende teenindamiseks kuluvat aega. Sellises olukorras aga tekib tagasiside, kus pikenenud vasteaeg suureneb paralleelselt vastust ootavate päringute hulka, mis omakorda suurendab vasteaega. Situatsiooni kujutab Joonis 7. Simulatsiooni kümnenda sekundini teenindab andmebaas kõik päringud nende saabumisega samas tempos ning igal hetkel teenindamist ootavate päringute hulk on stabiilne. Kümnendal sekundil aga toimub kasv ning andmebaasi vasteaeg hakkab pärast esialgset tõusu langema. Tipu lõppedes on andmebaasi võime päringuid teenindada jätkuvalt suurem, kui sisse tulevate päringute hulk ajaühikus (hall joon on kõrgemal, kui sinine) ning seetõttu hakkab vastust ootavate päringute hulk langema.[72] Süsteem taastub sisendi kõikumisest tagajärgedeta.



Joonis 8. Puhverdamata süsteemi käitumine pikema sisendkoormuse tipu korral

[71] Eeldatud on küllalt naiivset lineaarset vasteaja langust, reaalsetes tingimustes on vasteaja langus tõenäoliselt pigem eksponentsiaalne.
[72] Kujutage ette vanni: vanni veetase langeb, kui vanni voolab ajaühikus vähem vett, kui sealt välja voolab.

Kui tipp kestab liiga kaua, langeb andmebaasi vastevõime allapoole tavapärast koormusfooni ning süsteem ei taastu kunagi. Sellist olukorda kujutab Joonis 8. Vaid veidi eelmisest stsenaariumist pikema tipu korral langeb baasi vasteaeg alla tavapärast koormusfooni ning süsteem ei taastu enam sisendi kõikumisest.



Joonis 9. Puhverdatud süsteemi käitumine pika sisendkoorumuse tipu tingimustes

Süsteemiadministraatori vaatest on teenindavad süsteemid "punases", kuid koormus ei erine kuidagi tavalisest. Samuti taastub olukord pärast teenindavate süsteemide taaskäivitamist, sest paralleelsete sessioonide hulk langeb selle käigus uuesti normi piiresse.

Eraldi ära märkimist väärib andmebaasi vasteaja ja paralleelsete sessioonide hulga graafikute keeruline kuju vaatamata lihtsatele ning lineaarsetele sisendandmetele. On ebatõenäoline, et inimene suudaks kõrvalise abita hinnata nende täpset kuju konkreetse toodangusüsteemi puhul.[73] Teise olulise kahe stsenaariumi tunnusena tuleb tähele panna, et andmebaasi võime päringuid teenindada saavutab esmalt tipu ja hakkab siis kiiresti langema. Järelikult on andmebaasi vasteaeg allpool optimaalset ning päringud ootavad oma vastust liiga kaua. Kui andmebaasi vasteaeg õnnestuks hoida pidevalt optimaalsel tasemel, võiks sõnumite keskmine süsteemis veedetud aeg langeda ka siis, kui need veedaksid mõnda aega järjekorras oodates.

Sellist olukorda kirjeldab Joonis 9. Sisendkoormuse tipu saavutamisel asub andmebaas tööle optimaalsel võimsusel ja, kuna sessioonid ei oota enam mitte andmebaasiserveris, kus neid paralleelselt töödelda üritatakse, vaid järjekorras, kus nad ressurssi sisuliselt ei kuluta, siis andmebaasi vasteaeg jääb optimaalseks. Kuna sisendkoormus jätkuvalt ületab

[73] See eeldaks keeruliste diferentsiaalvõrrandite süsteemi numbrilist lahendamist ebaselgete väärtuste ning suurtes piirides kõikuvate parameetrite komplekti puhul.

andmebaasi võimet päringuid teenindada, siis paralleelsete sessioonide hulk (ehk järjekorra suurus) kasvab. Tipu lõppedes aga hakkab see kiiresti langema.

Simulatsioonid näitavad selgesti, et kiiresti muutuva sisendkoormuse puhul võimaldab päringute järjekorda ootama suunamine hoida taustasüsteemide jõudluse optimaalsena ning, mõnevõrra ebaintuitiivselt, lühendada keskmist päringute vasteaega. Veelgi enam, puhverdamata süsteemide puhul on võimalikud olukorrad, kus süsteem ei taastu kiiretest muutustest sisendis, millel kindlasti on halb mõju süsteemi käideldavusele ning seega ka vasteajale.

PROUD ENGINEERS

Lisa - Kasutuslugude ja komponentide seosed

Tabel 2. Primaarsete kasutuslugude ja komponentide seosed

	Digiallkirja teek	Dokumendihaldur	Eraisiku otsinguliides	Juriidilise isiku otsinguliides	Kasutajaliides	Konfiguratsiooni-haldur	Konfiguratsiooni-adapter	Muutmisadapter	Nimeadapter	Nimepuhver	Oraakel	Oraakliadapter	Rollihaldur	TARA	Uuendusadapter	Väliste rollide muutmise adapter
UC01. Kasutaja volitab isikut B isiku A suhtes rolliks X					X								X			
UC06. Kasutaja määrab eraisikust esindaja			X		X											
UC07. Kasutaja määrab juriidilisest isikust esindaja				X	X											
UC08. Kasutaja vaatab talle või tema esindatavale antud volitusi					X				X	X			X			
UC09. Kas isikul A on isiku B suhtes roll X?											X	X	X			
UC10. Kasutaja loobub talle või tema esindatavale antud volitusest					X								X			X
UC11. Kasutaja vaatab tema või tema esindatavate poolt antud volitusi					X				X	X			X			
UC12. Kasutaja eemaldab antud volituse					X								X			X
UC14. Kasutaja vaatab nimekirja isikutest, keda ta võib esindada					X				X	X			X			
UC15. Kasutaja vaatab nimekirja isikutest, kellele ta on andnud õiguse end esindada					X				X	X			X			
UC18. (Abstraktne) Kasutaja määrab esindaja																
UC22. Teavita rolli muutusest								X								
UC23. Uuenda seoste puhvrit																
UC24. Päri info seoste kohta															X	
UC30. Uuenda nimeruumi seadeid						X	X									
UC38. Kasutaja tuvastatakse					X									X		
UC42. Kasutaja allkirjastab volituse	X	X			X											
UC44. Kasutaja vaatab volituse aluseks olevat dokumenti		X			X											

	Digiallkirja teek	Dokumendihaldur	Eraisiku otsinguliides	Juriidilise isiku otsinguliides	Kasutajaliides	Konfiguratsiooni-haldur	Konfiguratsiooni-adapter	Muutmisadapter	Nimeadapter	Nimepuhver	Oraakel	Oraakliadapter	Rollihaldur	TARA	Uuendusadapter	Väliste rollide muutmise adapter
UC45. Roll aegub													X			

Tabel 3. Sekundaarsete kasutuslugude ja komponentide seosed

	Dokumendihaldur	Kasutajaliides	Muutmisadapter	Oraakel	Oraakliadapter	Rollihaldur	Soovituste hoidla	Väliste rollide muutmise adapter	Kasutajahaldur	OAuth liides	Sõnumiadapter	Soovituste haldur	TõRi adapter
UC13. Kasutaja teavitamine						X			X		X		
UC16. Kasutaja eemaldab kõik teda esindava isiku volitused		X				X		X					
UC20. Arvuta tuletatud rollid				X		X							
UC27. Lisa pääsuhalduse seos masinliidese kaudu	X		X			X							
UC28. Arvuta soovitused							X					X	
UC29. Kasutaja vaatab soovitusi järgmiste rollide lisamiseks		X					X						

	Dokumendihaldur	Kasutajaliides	Muutmisadapter	Oraakel	Oraakliadapter	Rollihaldur	Soovituste hoidla	Väliste rollide muutmise adapter	Kasutajahaldur	OAuth liides	Sõnumiadapter	Soovituste haldur	TöRi adapter
UC33. Eemalda pääsuhalduse seos masinliidese kaudu			X			X							
UC36. Kasutaja lisab volituse läbi OAuth voo						X				X			
UC37. Reageeri TöRi muutusele						X			X		X		X
UC41. Kasutaja muudab kontaktandmeid		X							X				
UC46. Kasutaja kopeerib isiku rollid		X				X							
UC48. Kasutaja loobub kõigist rollidest korraga		X				X							
UC49. Kasutaja muudab volitust		X				X							
UC50. Kasutaja otsib volituste nimekirjast või filtreerib volituste nimekirja		X				X							