TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Margus Sumla 204093IAAM

Identiteedi- ja juurdepääsuhalduse lahenduse täiendamine Tietoevry jagatud pilveteenuse keskkonna näitel

Magistritöö

Juhendaja: Nadežda Furs
MBA
Kaasjuhendaja: Edmund Laugasson
MSc

Tallinn 2022

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Margus Sumla

19.05.2022

Annotatsioon

Käesolev magistritöö käsitleb pilvarvutuse teenuse ligipääsuhalduse äri- ja IT protsesside analüüsi ning selle tulemusel püstitatud probleemi lahendamist uue infosüsteemi integreerimise kavandamise abil. Autor kirjeldab olemasolevat situatsiooni, analüüsib seda avalike allikate ja meetodite abil ning sellest lähtuvalt püstitab probleemi, mis väljendub ebaühtlase ja iganenud ligipääsuhalduse protsesside näol, millest tuleneb ressursside ebaefektiivne kasutamine.

Teenusepakkuja süsteemihaldurid on klientidele teenuse pakkumisega ajapuuduses ning uute klientide lisandumisel süveneb probleem veelgi enam. Töökoormus kasvab lisaks kasutajaõiguste haldamisele ka uute sellega seotud infosüsteemide osaliselt automatiseerimata juurutamise tõttu. Identiteedi- ja juurdepääsuhalduse süsteemi nõuete püstitamisega ja lahenduse kavandamisega kirjeldatakse uusi protsesse ja tehnilise lahenduse arhitektuuri, mille juurutamise abil on võimalik optimeerida töökoormust, kiirendada uute klientide pardaletulekut ja säästa kuludelt.

Lahenduse juurutamiseks vajalikud töö etapid on kirjeldatud ning planeeritud. Magistritöö tulemusi analüüsitakse püstitatud probleemi meetrika alusel, mis väljendub endas töötundide ning selle hinnangulise rahalise väärtuse näol.

Lõputöö on kirjutatud eesti keeles keeles ning sisaldab teksti 59 leheküljel, 6 peatükki, 20 joonist, 20 tabelit.

Abstract

Identity and Access Management Solution Improvement on the Example of Tietoevry in a Multitenant Cloud Service Environment

This master's thesis deals with the analysis of business and IT processes for access control of cloud computing services and designing the solution to the problem posed by the results by planning the integration of a new information system. The author describes the current situation, analyzes it with the help of public sources and methods and based on this raises a problem about uneven and legacy access management processes, which cause inefficient use of resources.

The service provider’s system administrators are short on time to provide services to the customers and the problem even escalates when there will be addition of new customers. The workload increases not only due to user rights management but also due to the partially non-automated implementation of new related IT systems. The description of the implementation of the proposed identity and access management system’s new processes and a technical solution architecture would be capable of optimizing the workload, accelerating the onboarding of new customers and saving costs.

The steps to implement this solution have been described and planned. The results of the thesis will be analyzed according to the metrics proposed in the raised problem, which is expressed in terms of hours worked and its estimated monetary value.

The thesis is in Estonian and contains 59 pages of text, 6 chapters, 20 figures, 20 tables.

Lühendite ja mõistete sõnastik

3C	*Card, Conversation, Confirmation*, kasutajalugude kvaliteedi määramise meetod
AC	*Acceptance Criteria*, nõuded, mille alusel IT arenduse kasutajalugu vastu võtta
AZ	*Availability Zone*, andmekeskus kõrgkäideldavuseks pilve regioonis
BPMN	*Business Process Model and Notation*, äriprotsesside modelleerimiskeel tegevuste visualiseerimiseks
CEO	*Chief Executive Officer*, tegevdirektor
CFO	*Chief Financial Officer*, finantsjuht
DAKI	*Drop, Add, Keep, Improve*, tagasivaatav ülevaate ja prioriseerimise meetod
FTE	*Full Time Equivalent*, täistööaja ekvivalent töömahu mõõtmiseks
FURPS	*Functionality, Usability, Reliability, Performance, Supportability*, infosüsteemide nõuete püstitamise ja analüüsi meetod
GDPR	*General Data Protection Regulation*, isikuandmete kaitse üldmäärus
HR	*Human Resources*, inimressurss (personaliosakond)
IaaS	*Infrastructure as a Service*, hallatud IT taristu teenus pilvarvutuses
IAAM	Infosüsteemide analüüs ja kavandamine, õppekava TalTechis
IaC	*Infrastructure as Code*, deklaratiivne virtualiseeritud andmekeskus
IAM	*Identity and Access Management*, identiteedi- ja juurdepääsuhaldus
IDaaS	*Identity as a Service*, hallatud identiteedi- ja juurdepääsuhaldusteenus pilves
IdP	*Identity Provider*, süsteemiväline identiteedi teenus integreerimiseks
IEC	*International Electrotechnical Commission*, elektriliste, elektrooniliste ja seotud tehnoloogiatele spetsialiseerunud standardiseerimise organisatsioon
INVEST	*Independent, Negotiable, Valuable, Estimable, Small, Testable*, kasutajalugude kvaliteedi määramise meetod
ISO	*International Organization for Standardization*, baasnõuetele vastavuse tunnustamise organisatsioon
JDBC	*Java Database Connectivity*, rakendustarkvara liides andmebaasidega ühendumiseks arvutivõrkudes
KPI	*Key Performance Indicator*, äriprotsesside võtmemõõdik
LDAP	*Lightweight Directory Access Protocol*, juurdepääsuõiguste võrguprotokoll
MVP	*Minimum Viable Product*, minimaalne elujõuline toode väärtuspakkumiseks

NAT	*Network Address Translation*, avalike-kohalike IP adressaatide suunamine
NPS	*Net Promoter Score*, kliendi rahuloluuuringu indeks
OIDC	*OpenID Connect*, OAuth 2.0 autoriseerimisprotokollil põhinev turvastandard ja turvaliste ühenduste loomise viis lisatud autentimisega
OLA	*Operational Level Agreement*, käitluslepe tugiteenuse osutaja ja teenuse vahel
RACI	*Responsible, Accountable, Consulted, Informed*, protsesside vastutusmaatriks
ROI	*Return Of Interest*, investeeringute tootlus
RSA	Rivest-Shamir-Adleman, asümmeetriline krüptoalgoritm turvaliseks andmevahetuseks
SaaS	*Software as a Service*, hallatud IT tarkvara teenus pilvarvutuses
SAFe	*Scaled Agile Framework*, agiilse tootearenduse karkass
SAML	*Security Assertion Markup Language*, autentimis- ja autoriseerimisprotokoll
SIPOC	*Suppliers, Inputs, Process, Outputs, Customers*, protsesside kaardistamisvahend ja analüüsi meetod
SMTP	*Simple Mail Transfer Protocol*, andmevahetusprotokoll e-kirjade edastamiseks arvutivõrkudes
SSO	*Single Sign-On*, mitmesse süsteemi sama kasutajakontoga autentimine
SWOT	*Strengths, Weaknesses, Opportunities, Threats*, strateegia ja konkurentsianalüüsi meetod
SLA	*Service Level Agreement*, teenustaseme lepe teenuse osutaja ja kliendi vahel
TLS	*Transport Layer Security*, turvaline andmevahetusprotokoll arvutivõrkudes
vh	*Viewport Height*, protsentuaalne mõõtühik nähtava veebilehe kuva suhtes
VPN	*Virtual Private Network*, turvaline ligipääs internetist privaatsesse sisevõrku
XaaS	*Anything as a Service*, mistahes IT komponendi hallatud teenus pilvarvutuses

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Identiteedi- ja juurdepääsuhaldus on reeglitest koosnev karkass, mille abil määratleda ja hallata organisatsiooni üksikute kasutajate ja seadmete ligipääsuõigusi. See aitab tagada, et vajalikel kasutajatel oleks juurdepääs vajalikele ressurssidele. Identiteedi- ja juurdepääsuhalduse abiga saab organisatsioon juhtida kasutajate ligipääsu töötajate, töövõtjate, partnerite jt kriitilisele teabele. [60]

Käesoleva magistritöö eesmärk on käsitleda identiteedi- ja juurdepääsuhalduse äri- ja IT protsesside kitsaskohtade määratlemist ja nende parendamise analüüsi organisatsiooni, meeskondade ja klientide vaatest Tietoevry (edaspidi organisatsioon või teenusepakkuja) pilvandmetöötluse äriteenuse suunal. Lähtuvalt organisatsiooni ja klientide nõuetest ning eripäradest analüüsitakse pilveteenuse juurutamisstrateegia ning identiteedi- ja juurdepääsuhalduse lahenduse erinevaid tüüpe. Olemasolevad protsessid on aegunud ning vajaks värskendamist ja klientide teenindusvõimekus on kasutatava süsteemiga piiratud.

Klientide juurdepääsuõiguste teenindamise maht on suurenevas trendis ja osaliselt käsitsi hallatav süsteem ning uute klientide juurdepääsu süsteemide juurutamine on ressurssidega piiratud. Olemasolevate klientide ja uute klientide lisandumisel tekib teenusepakkuja süsteemihaldurite kõrgendatud töökoormus, mida ei suudeta hallata.

Autor kirjeldab, modelleerib ja analüüsib probleemi taustsüsteemi, sellega seonduvat meetrikat ja pakub välja lahenduse, milles uue infosüsteemi analüüsi ja kavandamisega optimeeritakse olemasolevaid ning luuakse uusi protsesse. [5] Kavandatava süsteemi saavutatavaid tulemusi võrreldakse probleemi ja nõuete püstitusega ning tehakse tagasivaatavalt järeldusi.

Magistritöö sisaldab endas graafilisi jooniseid ja tabeleid, mis aitavad visualiseerida probleemi ja selle tausta, protsesside kulgu, töömahu arvulisi näitajaid, vastutavaid rolle ja võtmeprotsesse.

Magistritöö jaguneb kokku kuueks peatükiks, mille sissejuhatuse ja kokkuvõtte vahele jääv sisu jaguneb neljaks peatükiks ja nende alapeatükkideks.

Teises peatükis kirjeldatakse organisatsiooni ja pilveteenust pakkuva projekti tausta ning kirjeldatakse ja modelleeritakse olemasolevaid protsesse, keskendudes konkreetse probleemiga seonduvale.

Kolmandas peatükis analüüsitakse probleemi ning kirjeldatakse sellele vastavad mõõdikud, millele järgneb probleemi teoreetiline käsitlus ja protsesside ning tehnilise lahenduse analüüs.

Neljandas peatükis kirjeldatakse tehnilise lahenduse nõuete, protsesside parendamise ning nende optimeerimise kavandamist ja planeerimist töö etappide abil.

Viiendas peatükis analüüsitakse püstitatud probleemi lahenduse edukust ja mõõdetakse tulemusi.

Magistritöö lõpus paiknevad kasutatud kirjanduse loetelu ja lisad, mis sisaldavad endas jooniseid ja tabeleid ning lihtlitsentsi lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks. [5]

2 Tausta ja probleemi kirjeldus

Käesoleva peatüki ja selle alapeatükkide eesmärk on kirjeldada ja analüüsida probleemi taustsüsteemi. Tuuakse välja konkreetse organisatsiooni projekti infosüsteemi äriprotsesside ja infotehnoloogia omavahelisi seoseid, mis teineteist mõjutavad ja kirjeldatakse autori rolli antud projektis. Tuvastatakse ja analüüsitakse protsesse, mis piiravad ärieesmärkide saavutamise efektiivsust.

2.1 Organisatsioon ja ärikirjeldus

Tietoevry on 1968. aastal asutatud Põhja-Euroopa suurim täislahendusi pakkuv IT-ettevõte. Enam kui 24 000 spetsialisti 90-s eri riigis tegeleb innovatsiooni ja digitaliseerimise viimisega igasse elu- ja ärivaldkonda. Tietoevry missiooniks on infoühiskonna ehitamine. Oma tegevustes ollakse spetsialiseerunud suurte infosüsteemide loomisele, integreerimisele, hooldusele ja arendamisele. Tietoevry südameasjaks on luua digitaalne eelis ettevõtetele ja ühiskonnale. [1]

Tietoevry globaalne valitsemine ja juhtimine on hierarhilise struktuuriga, mille kihid jaotuvad järgnevalt.

- Juhtkond (*Board of directors*), mille liikmed valitakse osanike (*shareholders*) poolt aastaks ajaks [2] . Juhtkonna ülesandeks on lisaks organisatsiooni valitsemisele samuti selle presidendi ja tegevdirektori määramine [3] .

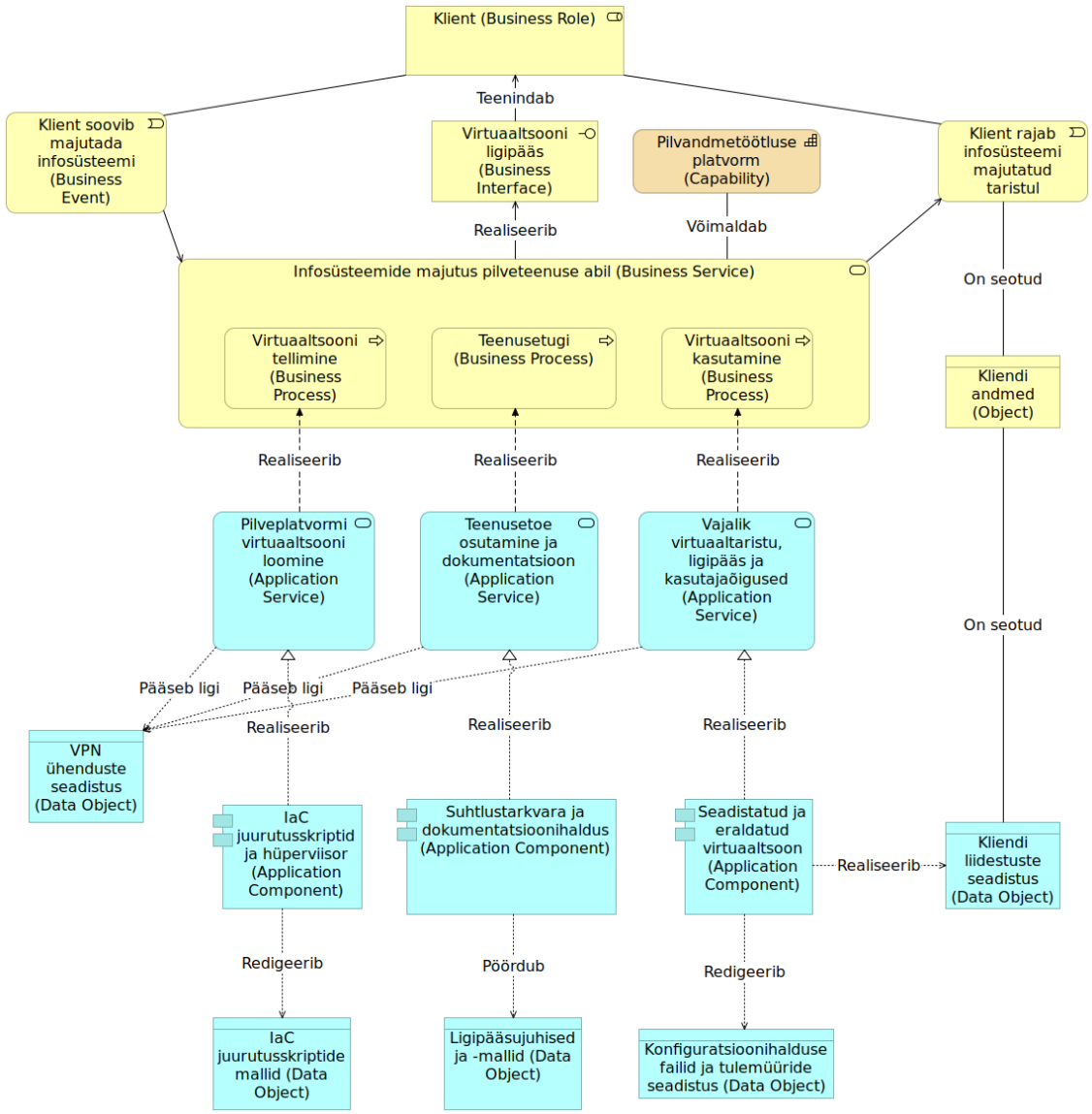
- President ja tegevdirektor (p*resident and CEO*), kes vastutab organisatsiooni toimimise juhtimise ning sisemise tõhususe ja kvaliteedi eest [3] .

- Tegevjuhtkond (*Country teams and service lines, heads of businesses, head of operations as well as head of HR, head of strategy and CFO*), mis vastutab presidendi ja tegevdirektori tegevuste toetamise eest, mille hulka kuuluvad muuhulgas protsessid ja kvaliteet, info- ja kommunikatsioonitehnoloogia,

hanked, ärihooned, strateegia, kommunikatsioon, bränd ja identiteet, jätkusuutlikkus, HR, õigus, finants, riskihaldus, privaatsus ja turvalisus. [4] , [Joonis 14]

Käesolevas magistritöös käsitletakse organisatsiooni konkreetset projekti, mis kuulub Tietoevry Create [17] ärisuuna alla ja tegeleb peamiselt infosüsteemide majutuslahenduste pakkumisega, võimaldades majutatavatel äriklientidel (*tenants*) pilveandmetöötluse tehnoloogial põhineval platvormil ärirakendusi luua ja käitada [5] . Infosüsteemide majutuse teenust pakutakse jagatud pilveteenuse keskkonnas, kus keskendutakse eelkõige kvaliteedile ja turvalisusele kui kvantiteedile. See tähendab, et pakutavate teenuste haldus on ajaliselt ja keerukuselt mahukad [2.3.2] ning teenindatav klientide arv piirdub magistritöö kirjutamise ajahetkel teenusepakkuja võimekuse tõttu ühekohalise arvuga. Joonisel [Joonis 1] on modelleeritud identiteedi- ja juurdepääsuhalduse äriteenuse realiseerimine.

Käesoleva projekti arendus- ja haldusprotsessid on kombinatsioon organisatsiooni väärtustest, SAFe'is kasutatavatest ja klientide endi kasutatavatest meetoditest. Organisatsioon hindab avatust ja usaldust, horisontaalset meeskonnasisest töödejuhtimist, agiilseid tarkvaraarenduse meetodeid, avatud lähtekoodiga tarkvara kasutamist, paarisprogrammeerimist ja informatsiooni jagamist, põhjalikku süsteemide testimist, DevOps põhimõtete rakendamist ning sisseehitatud turvet.



Joonis 1. IAM äriteenuse realiseerimise kihiline mudel

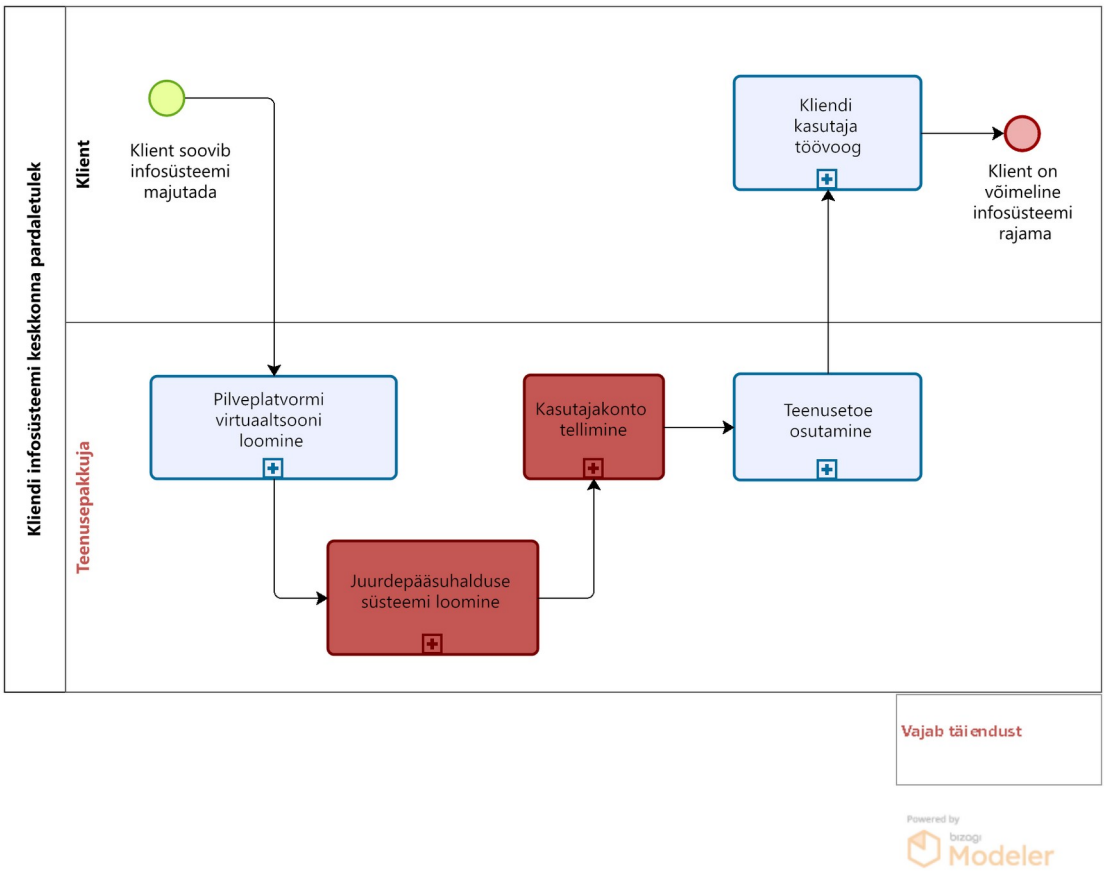
Kaasaegsed pilvandmetöötluse trendid viitavad sellele, et üha enam ettevõtteid majutavad enda äriga seotud infosüsteeme hübriid- ja mitmikpilves (*hybrid cloud and multi-cloud*) [6] , [Joonis 8]. Seesugused pilvarvutuse tehnoloogiad võimaldavad agiilsust [7] ja eraldada konfidentsiaalseid andmeid privaatse pilve või suveräänse pilve abil [8] ning tõsta süsteemide käideldavust liiasuse ja kättesaadavustsoonide abil (AZ) [9] , viies pilvarvutuse ressurssi geograafiliselt lõpptarbijale lähemale. Käsitletava projekti pilvandmetöötluse teenuse eelis kommertsiaalsete avalike pilveteenuse pakkujate ees on geograafiline asukoht, sest peamiseks sihtgrupiks on Põhjamaade organisatsioonid, milles on välistatud teatud andmete piiriületus. Samuti on eeliseks

kliendipõhine lähenemine, mis tagab paindlikkuse ja võimaldab klientidel hallata ning jätta teenusepakkujale hallata täpselt seesuguse osa infosüsteemist, mida soovitakse ja kokku lepitakse. [5]

2.2 Probleemi püstitus

Iga olemasoleva ja uue majutatava kliendi infosüsteemide arendus- ja haldusmeeskonnad vajavad teenusepakkuja pilveteenuse platvormi kasutamiseks ligipääsu. Joonisel [Joonis 2] on modelleeritud iga uue kliendi või uue kliendi infosüsteemi keskkonna pardaletuleku äriprotsessi, mis seisneb teenusepakkuja vaates vajaliku virtuaaltsooni loomises, ligipääsuõiguste seadistamises ja vastava teenusetoe osutamises. „Juurdepääsuhalduse süsteemi loomine" alamprotsess on puudustega, sest sisaldab endas liialt käsitsi tehtavaid toiminguid, mida on täpsemini kirjeldatud punktis [3.1].

„Kasutajakonto tellimine" alamprotsess on teenusepakkuja süsteemihalduritele liialt koormav, mille täpsemaid samme on kirjeldatud punktis [2.3] ja joonisel [Joonis 9]. Peamiselt sisaldab kasutajakonto tellimise täideviimine teenusepakkuja jaoks endas kliendi spetsialistide jt töötajate kasutajakontode ja -õiguste ning ligipääsude haldamist, et võimaldada kliendi kasutajatele pilveplatvormi kasutajaliidestesse sisse logimist ja süsteemide kasutamist. Kliendi kasutajate töövoog on osa äriprotsessist [Joonis 2], mida on modelleeritud joonisel [Joonis 15]. Ligipääsude tehnilist haldust tehakse vastava kliendi-spetsiifilise keskse ligipääsu süsteemis, mis tagab erinevate klientide loogilise eraldatuse platvormil tarkvaraliselt. Uue kliendi puhul tuleb keskne ligipääsu süsteem juurutada. [5]

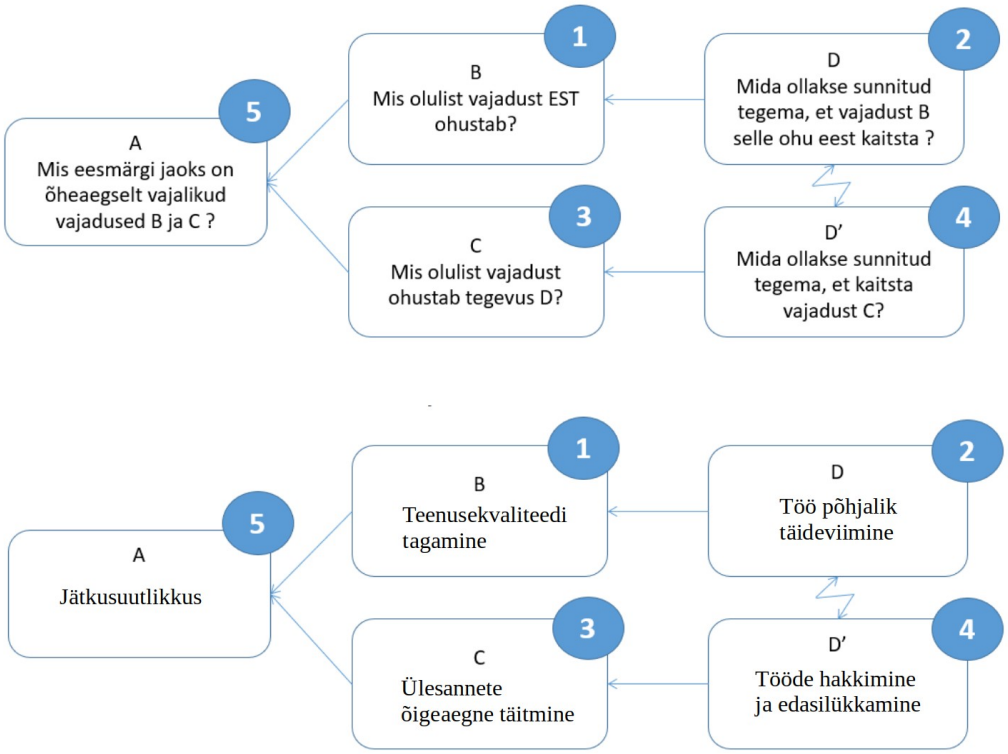


Joonis 2. Kliendi infosüsteemi keskkonna pardaletuleku äriprotsessi mudel AS-IS

Identiteedi- ja juurdepääsuhalduse tehniline kasutajaõiguste halduse läbiviimine teostatakse kahe meeskonnaliikme poolt [2.3.2]. Lisaks kasutajakontode haldusele kuulub sellega seotud tegevuste hulka ka autentimisteenuse serverite juurutamine, testimine ja ülalhoid [2.3.2], klientrakenduste seadistamise tehniline nõustamine kolleegidele, asjakohase dokumentatsiooni [2.3] koostamine iga virtuaaltsooni jaoks jt.

Teatavasti suureneb süsteemiadministraatori töömaht ajas seoses riistvara ja tarkvara uuendustega, andmemahtude suurenemisega jpt lisatoimingutega, ka ühe ja sama süsteemi haldamisel. Seetõttu on oodata üldkulude (*overhead*) suurenemist ning sama FTE tööaja väärtusega ei ole samal tasemel talitlus jätkusuutlik. See tähendab, et peamiselt ühe (autor) ja vajadusel kahe asjaosalise süsteemihalduri töökoormus suureneb märgatavalt. [19] See omakorda mõjutab äriliste eesmärkide saavutamist käesoleva projekti ning seega ka äriüksuse ja terve organisatsiooni jaoks ja vähendab

konkurentsivõimet, sest klientide arvu ja töömahu suurenemisel võib ennetada teenindusdefitsiiti, mis võib tingida kliendist loobumise või töökvaliteedi languse.



Joonis 3. Tööülesannete konfliktidiagramm

Tabelist [Tabel 1] ja jooniselt [Joonis 3] on näha, et teenindatavate klientide arvu kasvades suureneb juurdepääsuhalduse toimingutele kuluva aja ja seega kulutuste summa. Kuna iga kliendi jaoks on loodud eraldi autentimisteenuse serveripaar, siis toimub eelneva loetelu tegevuste mitmekordistumine. See võib tingida ka ülejäänud tööülesannete vahel rööprähklemise (*multitasking*) ja prioriseerimise, mis võib viia nende edasilükkamiseni ja seega teenuse kvaliteedi languseni, sest enam ei keskenduta tegevuste korrektsele täideviimisele vaid nende lõpetamisele. Seesuguste ebasoovitavate ilmingute vahel tekib konflikt, mis on modelleeritud joonisel [Joonis 3].

2.3 Ligipääsuhalduse töövoog ja osapooled

Kasutajakontode ja -õiguste ning ligipääsude haldus on järjepidev protsess, sest pilveteenuse platvormi arendatakse agiilselt – inkrementaalselt ja iteratiivselt. Ka klientide infosüsteemid on pidevas muutumises ning see toob endaga kaasa serverite ning funktsionaalsuste loomise ja hävitamise, kasutajate rollide muutumise, VPN ühenduste lubamise ja keelamise ning kasutajate informatsiooni (k.a paroolide) halduse jmt. Teenusepakkuja pakub kliendile väärtust võimalusega kasutada IaaS'i, mille abil enda infosüsteeme käitada ja arendada, mis omakorda on mõeldud kliendi enda ärilise eesmärgi tarvis. Klient loobub riistvara ja hüperviisori haldamisest ning ostab seda sisse (*outsource*), keskendudes peamiselt tarkvaralistele lahendustele alates operatsioonisüsteemi ja/või selle juurutamise haldamisest ning lõpetades rakenduste käitamise ja kasutajatele kättesaadavaks tegemisega. [10]

Identiteedi- ja juurdepääsuhalduse protsess seisneb töövoos, mida on võimalik läbi viia korratavate sammudega, sest eeldused ligipääsuõiguste lisamiseks on juba eelnevalt loodud. Kui kliendi kasutaja on saanud uue ülesande, näiteks juurutada käitatavale infosüsteemile uus funktsionaalsus F, mis töötab serveris S, siis on tarvis võimaldada talle kaughalduse ühendus, kuna server S asub teenusepakkuja pilveruumis ja on kättesaadav vaid turvalise internetiühenduse (VPN) kaudu. Järgnevalt kirjeldatakse standardse kasutajaõiguste päringu töövoo näidet teenusepakkuja vaatest [Joonis 9].

- Kliendi kasutaja loob sedelisüsteemis (*ticketing system*, nt ServiceNow, Jira või GitLab) uue päringu/tellimuse, milles kirjeldab enda identiteeti, tööpositsiooni, ülesannet, infosüsteemide keskkondade ja serverite parameetreid, kuhu on ligipääsu tarvis.

- Teenusepakkuja kliendihaldur otsustab või delegeerib otsustuse süsteemi alaosa eest vastutajale või kõrgemale juhtkonna tasemele, et kliendi kasutaja päring töösedelis kinnitada või tühistada. NB! See toimingu menetlemise aeg varieerub, sest klientide juurdepääsuõiguste tellimine ja haldamine ei ole ühtselt korraldatud.

- Kui töösedel on kinnitatud, siis avaneb teenusepakkuja süsteemihaldurite meeskonnaliikmetel võimalus kasutajaõiguste lisamisega alustada. NB! Selle töö tegemiseks planeeritud kvalifitseeritud ja ka privilegeeritud meeskonnaliikmed on piiratud.

- Kui üks teenusepakkuja süsteemihalduritest on töösedeli vastu võtnud, siis hallatakse kasutajaid ja nende õigusi rakendusega A (nt Apache Directory Studio, Jxplorer Java LDAP Browser, OpenLDAP [14] jpt).

- Seejärel on tarvis sisse logimise info, IP aadressid jmt juhised saata kliendi kasutajale käsitsi, redigeerides eelnevalt salvestatud e-kirja malle.

- Kui kliendi kasutaja on veendunud enda õiguste korrektsuses ja toimivuses, siis ta annab sellest teenusepakkuja süsteemihaldurile teada.

- Seejärel sulgeb teenusepakkuja süsteemihaldur töösedeli ja protsess on lõppenud.

Kasutajakonto ja/või -õiguste lisamisel on 3 aktiivset osapoolt ehk rolli, mida käesolevas magistritöös eristatakse, nähtav tabelis [Tabel 15]. Identiteedi- ja juurdepääsuhalduse töövoo sammudes osalevate rollide omavahelised seosed ning sisendid ja väljundid on kirjeldatud tabelis [Tabel 16]. Järgnevalt loetletakse käsitletava töövoo osapoolte kirjeldused ja eeldused.

- Kliendi kasutaja: organisatsiooniväline tarkvaraarendaja, projektijuht (k.a klientide alltöövõtja kasutajad) jmt, kes taotleb või kelle nimel taotletakse juurdepääsuõigusi teenusepakkuja pilveplatvormile. [5] Kliendi kasutaja eeldab teenusepakkujalt vastavaid juhendeid, mille abil ligipääsu taotleda. Need kliendile mõeldud juhendid peavad endas sisaldama kirjeldust taotluse esitamise vormi kättesaadavuse kohta, taotluse väljade selgitusi, kontaktisikute andmeid, eeldatavat menetlemise aega, informeerimist päringu menetlemise kulgemisest ja teavet teenusetoe saamise kohta.

- Teenusepakkuja kliendihaldur: organisatsioonisisene projektijuht või muu vanemtöötaja, kellel on õigus juurdepääsuõiguse taotlusi tellida (kinnitab ise), kinnitada või tagasi lükata teiste tellimusi ja samuti kinnitamise otsust

delegeerida. [5] Teenusepakkuja kliendihaldur eeldab, et talle on kättesaadavad kliendile mõeldud juhendid [2.3] ja lisaks teenusepakkuja süsteemihaldurilt päringu kinnitamise järel täideviimist niipea kui võimalik ning enda toimingutest õigeaegselt informeerimist kliendile kui ka kliendihaldurile endale.

- Teenusepakkuja süsteemihaldur: organisatsioonisisene süsteemi- või rakendusadministraator jt, kes teostab dokumentatsiooni halduse ja juurdepääsuõiguste tagamise tehniliselt. [5] Teenusepakkuja süsteemihaldur eeldab, et kliendile mõeldud juhendid [2.3] on neile kättesaadavaks tehtud ning et päringud saabuvad korrektse vormingu ja sisuga. Selle teabe põhjal lisatakse, muudetakse või eemaldatakse kasutajakonto ja sellega seonduvat informatsiooni ning ligipääsude õigusi ja saadetakse vastavad juhised ja teated.

2.3.1 Teenustaseme- ja operatiivtaseme lepe

Iga käsitletava projekti kliendi ja teenusepakkuja vahel on erinevad kokkulepped. Teenusel põhinevad SLA tasemed antud näites projekti kliendi X juures on pronks, hõbe ja kuld [11] , mis sätestavad erinevate parameetrite (sh teenuse tööaeg, käideldavus, tõrgete esinemise maksimaalne sagedus, reageerimisajad jt [12]) arvulised väärtused. Võttes vaatluse alla kliendi X uute kasutajaõiguste lisamise teenuse eeldatava tööaja, siis selgub, et see ei ole konkreetselt sätestatud. Autori poolt menetletud kasutajaõiguste lisamise töösedelite lahendamise tööaja väljadelt puudub väärtus ning protsess toimib suusõnalisel *best-effort* [16] põhimõttel, kus kliendi X kliendihaldur on väljendanud soovi kasutajaõiguste kättesaamiseks vaid töötundide ajal (9-17, E-R). Kliendi X puhul sobituks seesugune kokkulepe pronks SLA taseme alla.[1]

OLA puhul vastutavad piisava pädevuse ja süsteemiadministraatori juurdepääsuõigustega meeskonnaliikmed ligipääsude haldamise süsteemi rakenduste käideldavuse ja juurutamise eest. Praktiliselt peavad mainitud rakendused olema kättesaadavad töötundide ajal (9-17, E-R) ning erijuhtude puhul ka töövälisel ajal, kui selleks ajaks on planeeritud mõni kriitiline muudatus. Tegelikkuses puudub informatsioon käideldavuse aja kohta ning uute rakenduste juurutamine toimub suusõnaliselt kokku lepitud *best-effort* [16] põhimõttel.[2]

1 Autoril puudub ligipääs lepingutele ja kirjeldatakse vaid töösedelitel nähtavat.

2 Autor on üks juurdepääsuõiguste administreerijatest.

2.3.2 Tööhõive ja autori roll projektis

Käsitletava Tietoevry projekti infrastruktuur kui kood (IaC) platvormi arendus- ja haldusmeeskond (*DevOps* team), mille liige on ka autor, vastutab tarkvaralise andmeturbe, süsteemi alakomponentide automatiseerimise ning kõik teenusena (XaaS [26]) arenduse, käideldavuse ja ülalhoiu eest. Lisaks võimaldab vajaliku konfiguratsiooni, arvutivõrgu- ja õigustepõhise ligipääsu (IAM) ning pakub teenusetuge. [5]

Autori roll muuhulgas projekti tehnilise ülalhoiu tegevuste kõrval on platvormi juurdepääsuhalduse süsteemidega seonduv, mis ei hõlma endas vastutust IT arhitektuuri puudutavate otsusete tegemist. Otsused langetab IT arhitektuuri nõukogu [3.4.1], mille poole on võimalik probleemi kirjeldusega pöörduda mistahes meeskonnaliikmel. Autorit on käesoleva teemaga seonduvalt kaasatud IT arhitektuuri otsustusprotsessidesse, kui selleks on vajadus tekkinud.

Lisaks kasutajaõiguste haldusele [Joonis 9] vastutab autor meeskonnaliikmetele ja klientidele mõeldud juurdepääsuhalduse rakendusserverite terve elutsükli eest. Sinna hulka kuulub serverite ja rakendustarkvara automatiseeritud juurutamisskriptide uuendamine ja korrashoid, seadistuste käsitsi ja automatiseeritud testimine, rakendusserverite juurutamine, seadistamine, varundamine, taastamise testimine ja dokumenteerimine, utiliseerimine ja (turva)uuenduste paikamine.

Identiteedi- ja juurdepääsuhalduse süsteemiadministraatori toimingud ehk tehniline kasutajaõiguste halduse läbiviimine teostatakse kahe meeskonnaliikme poolt. Meeskonnasisese kokkuleppe kohaselt on autor peamine juurdepääsuhalduse küsimustega tegeleja ning tema kolleeg on abiks mahukamate probleemide lahendamisega ja kõrgenenud töömahu või puhkuse ajal asendusega. Töötajate täistööajast juurdepääsuhalduse tegevustele kulunud aritmeetiline keskmine aeg kliendi kohta on välja arvutatud töötundide arvestuse raportite ajaloo abil 1 aasta perioodil ja näidatud tabelis [Tabel 1] ja joonisel [Joonis 10].

Tabel 1. Kvalifitseeritud IAM töötajate FTE jaotus klientide vahel AS-IS [5]

	Klient 1	**Klient 2**	**Klient 3**	**Klient 4**	**Klient 5**	**Kokku**
Töötaja 1 FTE	0.1	0.2	0.1	0.15	0.05	**0.6**
Töötaja 2 FTE	0.2	0.4	0.1	0.3	0.1	**1.1**
Kokku	**0.3**	**0.6**	**0.2**	**0.45**	**0.15**	**1.7**

Kumuleeritud FTE-de arv kahe töötaja 5 kliendi arvestuses on 1.7[1], mis on võrdeline 272[2] töötunniga kalendrikuus. Eesti keskmise DevOps inseneri netokuupalga 2706[3] € [61] , mille tööandja kulu kokku on 4694[4] € [62] juures on 272 töötundi täiskohaga töötaja ettevõttele kulu 7979[5] € ulatuses kuus ja 95 748[6] € aastas.

2.3.3 Äri- ja IT strateegia

Kuna käsitletava projekti äristrateegia lähtub äriüksuse Tietoevry Create [2.1] strateegiast, mida tutvustatakse allüksustele ja projektide meeskondadele kinnistel sisemistel koosolekutel, siis toetub käesolev peatükk vaid avalikule teabele [18] . Tietoevry Create [2.1] keskendub pilvepõhiste lahenduste juurutamisele [17] ja seetõttu on eesmärgid otseselt seotud äriüksuse ja organisatsiooni strateegiaga. Oluliseks peetakse innovaatilise ja jätkusuutliku väärtuse loomist agiilselt, skaleeritavalt ja minimaalse turule jõudmise ajaga. [17]

1 $0.1+0.2+0.1+0.15+0.05+0.2+0.4+0.1+0.3+0.1=1.7$
2 $160 \cdot 1.7 = 272$
3 $(3874+1539)/2 \approx 2706$
4 $2706+1157.9+28+70+56+676 \approx 4694$
5 $4694 \div 160 \cdot 272 \approx 7979$
6 $7979 \cdot 12 = 95748$

Tabel 2. Tietoevry konkurentsianalüüs SWOT [15]

Tugevused (*Strengths*)	**Nõrkused (*Weaknesses*)**
1. Digitaalsete teenuste turuliider Norras, Rootsis ja Soomes. 2. Mitmekesine ülemaailmne võimekus kuue ärisuunaga portfoolio abil. 3. Tugev ja järjepidev rahavoo tekitamine.	1. Ärifookus on piiratud Põhjamaade piirkonnaga. 2. Kõrge võlatase teiste IT tööstuse konkurentidega.
Võimalused (*Opportunities*)	**Ohud (*Threats*)**
1. Tieto ja EVRY liitumisel tekkinud teineteist täiendavad ärid. 2. Strateegiliste partnersuhete laiendamine (näiteks Soome metsatööstus UPM). 3. Positiivne dünaamiline väljavaade Põhjamaade IT turule. 4. Põhjamaade ettevõtted soovivad areneda mitmikpilve keskkondadesse.	1. Cloud Hopper tüüpi rünnakud Managed Service Providers (MSP) suunal. 2. Valuutakursi negatiivne mõju äri kasvule. 3. Jäik konkurents Põhjamaade piirkonnas India IT teenusepakkujatega.

SWOT analüüs [Tabel 2] on tehtud organisatsiooniülese äristrateegia kohta ja sellest tulenevad ärieesmärgid on projektipõhiste ärieesmärkidega tihedalt seotud – projekti äristrateegia järgib organisatsiooni äristrateegia eesmärke. IT SWOT on jäetud eraldi käsitlemata, sest selle kohta avalik informatsioon puudub, kuid kuna IT teenuste pakkumine kuulub organisatsiooni põhiprotsesside hulka, siis leidub seal kattuvusi.

Äriteenuse motivatsioon ja strateegia on modelleeritud joonisel [Joonis 18], kus kaardistatakse äriliste eesmärkide saavutamiseks vajalikud osapooled, soovitavad tulemused, põhimõtted, nõuded, tegevussuunad, võimekused [Joonis 19] ja ressursid.

2.4 IT arhitektuur

Kliendile loodava väärtuspakkumise tehniliseks teostamiseks on tarvis määratleda IT arhitektuur. IT arhitektuur on oluline, sest see aitab ärieesmärke ja neid teenivaid IT lahendusi hoida omavahel sünkroniseerituna, luues kahe poole vahel ühiselt mõistetava vaate. Arhitektuurne vaade kujutab endast ülevaadet IT arhitektuurist, mis võimaldab seotud osapooltel (*stakeholder*) verifitseerida kuidas see probleemi lahendab. [51] IT arhitektuur väljendab süsteemi(de) komponente ja nende omavahelisi seoseid, mis aitab säilitada ühtset ja selget arusaama ning visiooni. Kui arendus- ja haldusmeeskondade töökorraldus, meetodite ja tööriistade valikud juhinduvad IT arhitektuuri järgi, siis on tõenäolisem, et saavutatavad tulemused on optimaalsed. IT arhitektuuri mõistmisega on ka piirangud ja võimalused arusaadavamad, mis aitavad säästa kuludelt, viia sisse muudatusi kiiremini ja veenduda komponentide omavahelistes seostes ja töökindluses. [52]

IT arhitektuuri valitsemine ja haldamine on kulukas, kuid see tasub ennast jätkusuutlikus projektis pikemas perspektiivis ära – „*If you think good architecture is expensive, try bad architecture.*" [53] IT arhitektuur jäljendab ettevõtte arhitektuuri hetkelist ja tulevast struktuuri ning käitumist, mis hõlmab endas samuti inimeste ja tehnoloogiate omavahelisi seoseid ja õigusi. [54] Identiteedi- ja juurdepääsuhalduse süsteemi IT arhitektuur on infotehnoloogiat kasutavas ja/või sellel põhinevas ettevõttes väga olulisel kohal, et eraldada turvaliselt teineteisest erinevate osakondade protsessid, süsteemid, inimesed ja andmed ning kiirendada töötajate tulemuslikkust väärtuse pakkumisel klientidele. [55]

Järgnevalt kirjeldatakse olemasoleva juurdepääsuhalduse lahenduse süsteemi olulisimaid komponente ja nende omavahelisi seoseid. Riistvara, andmekeskused, arvutivõrgu topoloogia, andmesalvestustehnoloogiad, hüperviisorid jmt IaaS ülalhoiuks vajalik madalama taseme IT taristu arhitektuur, mille eest autor ei vastuta [3.4.1], ei tule käsitluse alla, välja arvatud, kui sellel on otsene seos ja/või põhjus juurdepääsuhalduse lahenduse süsteemi toimimisel.

Olemasolev juurdepääsuhalduse lahenduse süsteem põhineb klient-server arhitektuuril, mille puhul autentimisteenuse server (serveriklaster) on keskne komponent ja

klientrakendused, mis selle teenust kasutavad, on arvutivõrkude abil hajutatud. Klientrakendused on kasutusel jagatud süsteemides, mida kasutavad isiklike kasutajakontodega projekti arendus- ja haldusmeeskonna liikmed ning kliendi kasutajad (kasutusel on näiteks hüperviisorid, hüppeserverid (*jump server*), andmebaasiserverid, logiserverid jpt). Klientrakendustele ligipääs tehakse kättesaadavaks turvalise teenuselüüsi abil, mis võimaldab välistest arvutivõrkudest ühenduda. Autentimisteenuse server on rajatud kahe virtuaalse rakendusserveri operatsioonisüsteemidele, et suurendada liiasuse (dubleerimise) abil tõrkekindlust ja käideldavust võimalike süsteemi- või ühenduvusprobleemide korral. Andmebaasid on nendesse serveritesse sisse ehitatud. [Joonis 16] Rakendusserverite juurutamine toimub parametriseeritud mallide (*template*) ja automatiseeritud skriptide käsitsi käivitamise abil. Skriptide abil on võimalik paigaldada ja seadistada serverite jaoks järgnevad tarkvara komponendid.

- Virtualiseeritud arvutivõrgu segmendid.
- Sissetulevate võrguühenduste tulemüüri seadistused kaughalduse ja juurdepääsuhaldusteenuse ligipääsuks.
- Väljaminevate võrguühenduste tulemüüri seadistused tarkvara ja uuenduste allalaadimiseks.
- RSA võtmepaari krüpteeritud turvalise kaughalduse autentimiseks.
- Virtuaalserveri koos ette määratud protsessori, muutmälu, püsimälu ja varunduse seadistustega.
- Operatsioonisüsteemi koos turbetarkvara, haldustarkvara ja konfiguratsiooniga.
- Autentimisteenuse serveri tarkvara koos ette määratud kliendi spetsifikatsioonidega (nimi, piirkond, tarkvara elutsükli keskkonnad, kasutajagruppide nimetused jmt).

Nende etappidega on esmane autentimisteenuse serverite paigaldus ja seadistus lõpetatud, kuid täieliku sobivuse saavutamiseks LDAP-i klientrakendustega integreerimiseks on tarvis veel lisaks käsitsi seadistusi teha, mida vaadeldakse lähemalt punktis [3.1].

3 Probleemi ja lahenduse analüüs

Käesoleva peatüki ja selle alapeatükkide eesmärk on kirjeldada ja analüüsida probleemi püstitust [2.2] ning nõuded [3.4], mille osakaal oleks mõõdetav [3.2]. Pakutakse välja lahendus, et automatiseerida ja optimeerida käsitsi tehtavaid toiminguid [3.1], mis võimaldaks teenusepakkuja süsteemihaldurite töökoormust vähendada.

3.1 Käsitsi tehtavad toimingud

Klientide virtuaaltsoonide ligipääsuhalduse süsteemide juurutamine on osaliselt automatiseeritud. Lisaks skriptide käsitsi käivitamise abil [2.4] paigaldatud ja seadistatud autentimisteenuse serveritele on tarvis teha veel käsitsi lisaseadistusi, mida automatsioon magistritöö kirjutamise ajahetkel endas ei hõlma. Need tegevused loendatakse järgnevalt.

- Autentimisteenuse serveripaari arvutivõrgu ühenduste turvamine TLS-i abil.
- Autentimisteenuse serveripaari andmebaasides sisalduvate kasutajaandmete automaatne omavahel sünkroniseerimine.
- Iganenud ja vähemturvaliste krüptoalgoritmide keelamine.
- Minimaalsete paroolinõuete määramine.
- Virtualiseeritud koormusjaoturi (*Load Balancer*) paigaldamine ja seadistamine selleks, et klientrakendused oleksid võimelised kasutama kõrgkäideldavat autentimisteenuse serveri teenust, kui on võimalik sisestada vaid 1 IP aadress või serveri nimi, mitte mõlemad.

Ligipääsude konfigureerimiseks hallatakse kasutajaid ja nende õigusi rakendusega A [2.3], [Joonis 9], mille abil ühendutakse soovitud kliendi virtuaaltsooni kasutajate ja õiguste rakenduse andmebaasi. Selle jaoks on vajalik VPN ühenduse loomine kliendi

virtuaaltsooniga ja seejärel korrektse IP aadressi, võrgupordi ja kasutajanime, parooli ning TLS turvasertifikaadi abil sisse logimine. Õiguste lisamine toimub graafilises keskkonnas kasutajakonto objekti lisamisel kasutajagruppidesse *copy-paste* põhimõttel ning sellele järgneb e-kirja koostamine ja selle teate käsitsi saatmine kasutajale tema uute õiguste kohta. Lisaks on tarvis ka kontosid sulgeda, õigusi eemaldada ning paroole taastada. [5]

Kui vaadelda standardse kasutajaõiguste päringu töövoo [2.3] kasutajakonto ja/või -õiguste lisamist ja nende kommunikeerimist kliendi kasutajale, siis on märgata, et need etapid on ebaefektiivsed ja võivad põhjustada osapooltele tööde hakkimist [Joonis 3]. Kasutajaõiguste teenindussoovi päringust kättesaamiseni töövoog ei ole järjestikune ning nõuab mitme inimese vahelist suhtlust. Võivad tekkida viivitused seoses erinevate tööpäeva alguse- ja lõpuaegadega, teabe puudujääkidega, inimvigadega, arusaamatustega erinevate klientide harjumuspäraste töövoogudega, tehniliste probleemidega jmt.

3.2 Probleemi mõõtmine

Identiteedi- ja juurdepääsuhalduse ja ka teiste infosüsteemide tulemuslikkuse mõõtmisel on lihtne teha valearvestusi. Süsteem juurutatakse üldistatud põhimõtete järgi, näiteks, et see peab teenindama servereid autentimise ja autoriseerimise funktsioonidega turvaliselt ja mugavalt. Tegelikkuses ei ole püstitatud konkreetseid eesmärke, mida silmas pidada, kui arvutatakse rahalist väärtust, mida see ärile toodab. [20] Mõned näited mõõdetavate KPI-de kohta identiteedi- ja juurdepääsuhalduse süsteemides.

- Äririskid, mis võivad tekkida, kui töötaja vallandamise ja ligipääsuõiguste järjekord ei ole kokku lepitud või kui kasutajakontod, mis ei ole justkui kellegi omad, aga võimaldavad süsteemidesse siiski ligipääsu. [20]

- Äritegevus, mille puhul on võimalik jälgida töötajate produktiivsust ja täiendada kitsaskohti, kui näiteks paroolide vahetamine või ligipääsude hankimine on liialt ajakulukas ning seega saaks optimeerida kulusid. [20]

- Turvalisus, mis hõlmab endas ligipääsude konfiguratsiooni peenhäälestust ja peab tagama, et kellelgi poleks liiga palju kasutajaõigusi ja nad ei pääseks

sellistesse süsteemidesse, milles neil autorisatsioon puudub. [20] Infosüsteemi identiteetide ja juurdepääsude omavahelised seosed on tehniline realisatsioon inimsuhetest organisatsioonis. Seda, nagu ka teisi süsteeme, ei ole võimalik üks ühele modelleerida – *„All models are wrong, but some are useful.”* [21]

- Kliendisuhted, mis võimaldavad jätkusuutlikku ärisuhet, kui kasutajakogemust hinnatakse ja püütakse seda täiendada. [20]

- Regulatiivsele ja seaduslikele nõuetele vastavus, mis võimaldab auditeerimise nõuetele vastavuse ning rahvusvaheliste standardite (ISO) ja sertifikaatide abil tunnustuse. [22]

Kuna identiteedi- ja juurdepääsuhalduse tööde tegemiseks planeeritud kvalifitseeritud ja ka privilegeeritud meeskonnaliikmete aeg on piiratud, siis ületatakse teatud uute klientide lisandumise ja kasutajaõiguste päringute arvu korral teenindamise võimekus [Tabel 1], [Joonis 10]. Mõõdikud ja KPI-d, mille abil käesolevat probleemi defineerida on järgnevad.

- Inimvigade arvust tingitud lisakulud käsitsi õiguste (*copy-paste*) lisamisel.

- SLA rikkumisest tingitud trahvisummad.

- Lisakulud, mis on tingitud ajalisest viitest teenusepakkuja ja kliendi vahelise informatsiooni käsitsi vahetamisel.

- Inimvigade arvust tingitud lisakulud autentimisteenuse serverite käsitsi konfigureerimisel.

- Inimese (võrreldes masinatega) aeglasest tööloomust tingitud lisakulud autentimisteenuse serverite käsitsi konfigureerimisel.

- Müügitehingute arv, mis on tingitud uute klientide juurdepääsu süsteemi juurutamise võimekusest.

- Lisakulud teenusepakkuja süsteemihaldurite töö hakkimisest, mis põhinevad kasutajahaldusega seotud toimingute ebakorrapärasest ilmnemisest.

Teenusepakkuja süsteemihaldurite töömaht oleneb veel lisaks kliendi töömahtudest ning päringute sagedusest ja süsteemi konfiguratsioonist. Klientide töömahu ja/või klientide arvu suurenemisel tõuseb teenusepakkuja süsteemihaldurite töömaht ning võib väljuda kontrolli alt [Tabel 1], [Joonis 10]. Kasutajate loomise ja juurdepääsuõiguste lisamise tehniline protseduur kestab keskmiselt 10 – 15 minutit. Virtuaaltsooni ligipääsuhalduse süsteemi pardaletulek kestab viimase 3 aasta statistika põhjal keskmiselt kuni 2 nädalat, kui välja arvata arvutivõrkude ja muu taristu ettevalmistused.

Kliendi rahulolu ja kasutajakogemuse mõõtmiseks koostas autor küsimustiku, mille palus täita kahe kliendi kasutajatel. Tulemused kajastatakse tabelis [Tabel 20]. Küsimuste 1 – 5 vastused on kvantitatiivsed. Kvantitatiivsete tulemuste põhjal on kasutatud kliendi rahuloluuuringu indeksit (NPS), mis võimaldab seada aluseks meetrika, et hinnata ja mõõta kliendi rahulolu teenuse kasutamisel. NPS-i arvutamisel lahutatakse 9 ja enam hinnanud vastanute protsendist 6 ja vähem hinnanud vastanute protsent. [66] NPS-i koguväärtuseks küsitluse tulemusel on 0, mis on neutraalne väärtus, kuid eelistatud oleks positiivne väärtus, mis on ka eesmärgiks seatud.

3.3 Probleemi käsitlus maailmas

Kuna kaasaegsed pilvandmetöötluse trendid viitavad sellele, et üha enam ettevõtteid majutavad enda äriga seotud infosüsteeme hübriid- ja mitmikpilves [2.1], [6] , [Joonis 8], siis juurutatakse ka identiteedi- ja juurdepääsuhalduse süsteemid pilvepõhiselt, sest see võimaldab IDaaS teenust sisse osta (*outsource*'ida) ja tsentraliseeritud lahendust kasutada interneti vahendusel, vähendades sellele kuluvat ressurssi [24] . Peamiselt kasutatakse kolme tüüpi identiteedi- ja juurdepääsuhalduse juurutusplaani.

- Majasisene (*on-premise*), mis on sageli ressursikulukas, kuid teatud organisatsioonide puhul turbenõuete tõttu vältimatu ning seda on võimalik panna sobituma organisatsiooniga. [23]

- Pilvepõhine (avaliku pilve) ehk majaväline (*off-premise*), mis on halduskulude poolest soodsam, kuid osade organisatsioonide puhul jääb küsitavaks konfidentsiaalsete andmete käitlemine ning avalike pilvede paindumatus, mis

tähendab, et organisatsiooni juurdepääsuhalduse nõuded tuleb selle järgi sobituma panna. [23]

- Hübriidpilvepõhine, mis võimaldab lahenduse soovidekohast paindlikkust, kuid suurendab ka süsteemiintegratsioonide keerukust. [23]

Privaatpilves majutatava infosüsteem identiteedi- ja juurdepääsuhalduse võib juurutada mistahes mainitud kolme erineva juurutusplaani [3.3] vahel, vastavalt eesmärgile ning konfidentsiaalsustasemele[1]. Kui infosüsteemi majutatakse avalikus pilves, siis on ka otstarbekas sama teenusepakkuja juures identiteedi- ja juurdepääsuhaldus seadistada, sest see sobitub pakutavate vahenditega. Hübriidpilv hõlmab endas eelnevalt mainitud stsenaariumite kombinatsioone, teenusepakkuja ja kliendi kokkulepetest sõltuvalt. [28] Valikut identiteedi- ja juurdepääsuhalduse väljakutsetest hübriidpilvede kasutamisel kirjeldatakse järgnevalt.

- Liigne kasutajakontode ja paroolide kasutamine, mis tekitab kasutajatele erinevate rakenduste sisse logimisel lisakeerukust. [27]

- Käsitsi kasutajaõiguste loomine ja eemaldamine süsteemidest, millega kaasneb kõrgendatud vigade tekkimist oht. [27]

- Ligipääsude kehv nähtavus, mis ei takistab saama selget arusaama kes pääseb kuhu süsteemile ligi. [27]

- Ligipääsusüsteemide andmesilod ehk -hoidlad, mis tekitavad liigse keerukuse ja kasutamata ehk raisatud kasutajaõiguste kogumeid. [27]

- Kaugtöö ligipääsude haldamine, mis tekitab olukorra, kus ligipääs süsteemidele peab olema lubatud terve maailma avalikest arvutivõrkudest. [27]

- Klientrakenduste integreerimise ajakohasena hoidmine, mis on hajutatud suuremahuliste süsteemide puhul keerukas. [27]

- Erinevad haldusmudelid erinevatele klientrakendustele, mis nõuavad haldusrakenduselt universaalsust. [27]

1 Teatud riigiasutuste, pankade jmt andmed tohivad paikneda vaid kindlas geograafilises piirkonnas.

- Mitteoptimaalne pilveteenuste kasutamine ja parimate praktikate ülevaate vähesus, mida identiteedi- ja juurdepääsuhalduse süsteemid saaksid sisse logimise ja süsteemide kasutamise informatsiooni abil toetada. [27]

- Järjepideva majasisese (*on-premise*) ja pilvepõhiste rakenduste ligipääsu haldamine, mis tekitab erinevaid kasutajakontosid ja -õigusi. [27]

Kuna kaasaegsetes ettevõtete infosüsteemide majutustrateegiates on jätkuvalt probleemne majasiseste andmekeskuste ja avalike pilvede kombineerimise meetod, siis on avalike pilveteenuste pakkujad välja pakkunud lahenduse juhttasandite (*control plane*) näol. Selle tehnoloogia abil on võimalik hallata näiliselt avalike pilvede poolt pakutavat teenust, kuid tegelikkuses on soovi korral andmed talletatud privaatselt ja majasiseselt. See võimaldab paigaldada ja kasutada erineval riistvaral ja ka teiste teenusepakkujate hüperviisoritel teenusepakkuja poolset pilveplatvormi hüperviisori haldustarkvara, mida ettevõtte IT spetsialistid on õppinud avalikes pilvedes kasutama. Seesuguse lahenduse abil on võimalik mugavamalt hallata mitmikpilve omavahelisi integratsioone, mis on jätkuvalt tõusev trend [2.1]. [35]

3.4 Loodava lahenduse analüüs

Käesoleva alapeatüki eesmärk on kirjeldada, analüüsida ja koostada probleemi püstitus ning kirjeldada äri- ja süsteeminõuded, et pakkuda välja lahendus, mis võimaldaks automatiseerida ja optimeerida käsitsi tehtavaid toiminguid [3.1]. Tulemused peavad olema mõõdetavad [3.2].

3.4.1 Analüüsi skoop ja piirangud

Kuna autor on osa meeskonnast ning liitus sellega siis, kui osa identiteedi- ja juurdepääsuhalduse süsteemi planeerimisest ja analüüsist oli juba tehtud, siis on tarvis määratleda skoop, et selgitada välja, mis on autori panus käesolevas magistritöös. Analüüsi skoopi kuulub ja autori panus on järgnev.

- Loodava tehnilise lahenduse funktsionaalsete ja mittefunktsionaalsete nõuete ettepanekute ülevaade, mis sisaldab endas meetodite ja standardite analüüsi ning võrdlemist.

- Andmekaitse ja andmeturbe parima praktika ja organisatsiooni huve teeniv kirjeldus.
- Uue täiendatud identiteedi- ja juurdepääsuhalduse teenuse protsessi kavandamine.
- Identiteedi- ja juurdepääsuhalduse delegeeritud administraatori õigustega teenuse pakkumise protsesside käsitlus projekti klientide vanemtöötajate ja kasutajate kohta.
- Epikute, kasutajalugude ja vastuvõtukriteeriumite analüüs ja ettepanekud funktsionaalsuste välja arendamiseks.
- Teoreetilise kliendi infosüsteemi kasutajagruppide kavandamise näited.
- Lahenduse tehnilise juurutamise kavandamise kirjeldus.
- Püstitatud probleemi teoreetilise lahendamise tulemuste analüüs.

Käesolevas magistritöös kirjeldatakse olemasolevat situatsiooni organisatsiooni projekti ja klientide vahel, seda analüüsitakse avaliku teabe abil ning leitakse organisatsiooni projekti võimekustele [Joonis 19] vastav lahendus. Pakutava pilveteenuse toimimise eest vastutab palju töötajaid ja järgnevalt väljendatakse nende töötajate kohustused ja eeltöö, mis käesolevasse magistritöös käsitluse alla ei tule. Järgnevalt kirjeldatakse, mis analüüsi skoopi ei kuulu ja milles autori panus on kaudne või olematu.

- Klientide ja teenusepakkuja vaheliste lepingute kirjeldus ja sisu.
- Riistvara, andmekeskused, arvutivõrgu topoloogia, andmesalvestustehnoloogiad, hüperviisorid jmt IaaS ülalhoiuks vajalik madalama taseme IT taristu arhitektuur, mille eest autor ei vastuta.
- Klientide töösedelite kasutamise viisid, sest teenusepakkuja vaates ei ole teada ega ka oluline, mis meetodil klient kasutajaõiguste päringuid koostab.
- Identiteedi- ja juurdepääsuhalduse lahenduse täiendamise tarkvarakomponentide valik ja nimetused, sest seda informatsiooni ei soovita avaldada.

- Infoturbe ja küberturbe käsitlemine (NB! see eristub andmekaitsest ja andmeturbest [36] , [3.5]).
- Identiteedi- ja juurdepääsuhalduse protsesside käsitlus organisatsioonisiseste töötajate kohta.
- Otsene rahaline mõõde püstitatud probleemi ja selle lahendamise tulemusest.
- Loodava tehnilise lahenduse detailne nõuete kirjeldus, sest komponendid on eelnevalt valitud.
- Loodava tehnilise lahenduse seire analüüs ja kavandamine.
- Loodava lahenduse teenustaseme- ja operatiivtaseme lepe.
- Automaattestide ja tarneahelate tehniline kirjeldus.
- Muudatushalduse protsessi kirjeldus uue lahenduse jaoks.
- Olemasolevate kasutajakontode migreerimise protsess.
- Mitmetasemelise autentimise ja paroolide keerukuse nõuete püstitamine ja analüüs.

Magistritöö kirjutamise ajahetkel, autorile teadmata põhjusel, ei ole meeskonnaliikmeid juurde palgatud, kuigi on näha, et töökoormus on kasvava loomuga [2.2], [Joonis 10].

Käesoleva projekti IT arhitektuuris on välistatud avalike pilvandmetöötluse keskkondade poolt pakutud ligipääsude süsteemide kasutamine regulatoorsetel ja seaduslikel põhjustel, sest kasutajaandmed peavad olema talletatud vaid privaatpilve tagaserverite andmebaasides. Samuti on nõutud avatud lähtekoodiga tarkvara [2.1] kasutamine, mis on sätestatud projekti IT arhitektuuri nõukogu poolt, põhjused on järgnevad.

- Iseseisva ülalhoiuga (*self-hosted*) identiteedi- ja juurdepääsuhalduse lahendus, millega on võimalik projekte integreerida, antud projekti puhul on oluline klientide andmed talletada lokaalselt.

- Turvalisuse kaalutlusel, sest avatud lähtekoodiga tarkvara vigade ja turvaaukude tuvastamise protsess toimub tunduvalt kiiremini ja efektiivsemalt, kuna sellega on võimalus kõigil huvilistel tutvuda [13] . Kommertstarkvara kasutamisel tuleb kasutajal teavitada arendajat veast, arendaja peab kinnitama vea, leidma lahenduse, katsetama seda ning seejärel väljastama paranduse. Selline protsess võib võtta nädalaid või kuid, mis võib tekitada ettevõttele kahju. Lisaks piiravad paljud kommertstarkvara litsentsid ja suletud lähtekood iseseisvate paranduste või täienduste tegemist. [13]

- Modulaarsuse ja dünaamilisuse tõttu, sest avatud tarkvara abil on võimalik seda vajadusel privaatpilve eripäradega kohandada ja sobituma panna.

Osade klientide puhul on lisatingimuseks Tietoevry pakutav suveräänse pilve teenus [25] , mida rakendatakse samuti käesolevas projektis, mille puhul peavad jääma klientide andmed nõutud riigipiiride sisse.

3.4.2 Funktsionaalsed nõuded

Selleks, et organisatsioonid saaksid kindlaks teha oma identiteedi- ja juurdepääsuhalduse süsteemide tõhususe, on tarvis kõigepealt hinnata, mil määral nende kasutusele võetud süsteemid vastavad funktsionaalsetele nõuetele. Lihtsamalt öeldes: kas need IAM-süsteemid teevad seda, mida organisatsioon ja selle kasutajad vajavad? Seetõttu on vajalik ja loogiline määrata kindlaks funktsionaalsed nõuded enne loodavate IAM süsteemide omaduste ja funktsioonide hindamist. [32] Funktsionaalsete nõuete määramiseks on tarvis mõista, missugused protsessid on kasutusel. Valik identiteedi- ja juurdepääsuhalduse süsteemi võtmeprotsessidest kliendi elutsükli jooksul loetletakse[1] järgnevalt.

- Kasutajakontode loomine, mis sisaldab endas kasutajakontode lisamist süsteemi. [34]

- Autentimine, mis sisaldab endas sisse logimist ning kasutaja ja rolli valideerimist. [34]

- Autoriseerimine, mis sisaldab endas ligipääsu lubamist ja jälgimist. [34]

1 Paljud nõuded on kirjeldatud ISO 27001 dokumendis, millest rohkem punktis [3.4.3].

- Iseteenindus, mis sisaldab endas kasutaja teabe ja seadistuse muutmist (isiklikud andmed jmt) ning parooli taastamist. [33]

- Paroolide haldus, mis sisaldab endas paroolinõuete ja -reeglite määramist. [33]

- Kasutajasessiooni haldus, mis sisaldab endas reaalajas logimist, kasutaja ligipääsu jälgimist ja vajadusel muutmist ning auditeerimist ja raporteerimist. [33] , [34]

- Kasutajakontode sulgemine, mis sisaldab endas ligipääsu eemaldamist ja kasutajakontode sulgemist. [33]

Tabelis [Tabel 17] defineeritakse funktsionaalsed nõuded epikute (*epic*) ja kasutajalugude (*user story*) abil lähtuvalt kasutajaõiguste halduse osapoolte [2.3] eeldustest. Funktsionaalseid nõudeid on otstarbekas epikute ja kasutajalugude kaudu kirjeldada, sest need on kirjas arusaadavate lausetena nii tehnilistele kui äripoole töötajatele. [46] Samuti kasutatakse seesugust lähenemist käesolevas projektis SAFe [2.1] karkassi abil.

- Mina teenusepakkujana soovin automatiseeritud lahenduse abil juurutada süsteeme, mis võimaldavad klientide eraldatud virtuaaltsoonide kaupa delegeerida identiteedi- ja juurdepääsu haldusrakenduste administreerimise õigust kliendi vanemtöötajatele, et vähendada töökoormust käsitsi tehtavate toimingute arvelt iga kliendi tarbeks – epik 1.

- Mina kliendi vanemtöötajana soovin kasutajaõiguste päringuid kinnitada või tagasi lükata ning hallata majutatavas infosüsteemis identiteedi- ja juurdepääsu haldusrakenduses enda organisatsiooni kasutajaid ja nende kasutajaõigusi virtuaaltsoonide keskkondade kaupa, et saaksin kasutajaõiguseid hallata organisatsioonisiseselt – kiiremini ja mugavamalt – epik 2.

- Mina kliendi kasutajana soovin kasutada identiteedi- ja juurdepääsu haldusrakenduses iseteenindust, et saada ülevaadet enda isiklikest andmetest ja kasutajaõigustest ning muuta ja taastada iseseisvalt parooli – epik 3.

Epikud ja kasutajalood keskenduvad pigem featuuride (*feature*) ning süsteemi spetsiifilistele alaosadele ja funktsioonidele, mitte süsteemile kui tervikule ning ei ole mõeldud konkreetsete ülesannete kirjeldamiseks. [46] Epikute ja kasutajalugude abil on ka võimalik mittefunktsionaalseid nõudeid kirjeldada, kuid seda ei peeta parimaks praktikaks, kuna tehniliste kasutajalugude määratlemine ärilise väärtuse kaudu on keerukas. [46] Epikud koostatakse käesoleva lahenduse protsessi osapoolte rollide kaupa järgnevalt ja analüüsitakse põhjalikumalt punktis [4.2].

3.4.3 Mittefunktsionaalsed nõuded

Kui funktsionaalsed nõuded vastavad küsimusele „kuidas?" süsteem peab toimima ja „mida?" tegema, siis mittefunktsionaalsed nõuded vastavad küsimusele „kui hästi?" see peab seda tegema. Mittefunktsionaalsed nõuded keskenduvad pigem süsteemile kui tervikule, mitte süsteemi spetsiifilistele alaosadele ega konkreetsete ülesannete kirjeldamisele. [46]

Autori esialgne kavatsus oli püstitada loodavale identiteedi- ja juurdepääsuhalduse lahendusele mittefunktsionaalseid nõudeid FURPS või FURPS+ meetodi abil, mis võimaldaks analüüsida ja mõõta vastava infosüsteemi kasutatavust, töökindlust, jõudlust ja toetatavust[1] [37] . FURPS-i kasutamisest identiteedi- ja juurdepääsuhalduse süsteemide puhul ei leitud autori otsingute järel avalikest materjalidest põhjapanevaid kirjutisi ning seega ei ole võimalik lisada selgitustele juurde tõestust.

Järgnev tabel [Tabel 3] on loodud autori kogemuse ja teadmiste põhjal sobimaks käesoleva projekti identiteedi- ja juurdepääsuhalduse teenuse süsteemiga kliendi kasutaja [2.3] ja kliendi [3.4.2] vaatest. Infosüsteemi tehnilisest kirjeldusest kirjutatakse lähemalt punktis [4.3].

1 Funktsionaalsuse nõudeid käsitletakse eraldi punktis [3.3].

Tabel 3. Loodava lahenduse mittefunktsionaalsed nõuded FURPS+ abil

Kasutatavus (*Usability*)	▪ Sisse logimise eelne ja sellele järgnev vaade peavad sisaldama selgelt ja nähtavalt informatsiooni, mis kliendi ja selle infosüsteemi elutsükli keskkonna virtuaaltsooniga on tegemist – minimaalselt 3 vh (*viewport height*) teksti suurusega. ▪ Unustatud sisse logimise parooli taastamise informatsioon peab olema välja saadetud kasutaja seadistatud e-posti aadressile maksimaalselt 10 sekundi jooksul.
Töökindlus (*Reliability*)	▪ Kasutajate- ja õiguste haldusteenus peab olema klientidele kättesaadav 99.99% ajast, mis võimaldab 13.15 minutit maasoleku aega kvartalis tarkvarauuenduste tegemiseks. ▪ Esirakenduse andmekao juhul peavad andmed olema taastatavad tagasüsteemi andmebaasist või selle varundusest.
Jõudlus (*Performance*)	▪ Kõik registreeritud kasutajad peavad olema võimelised teenust samaaegselt kasutama, häirimata teineteise kasutajakogemuse kvaliteeti. ▪ Rakendusserverite jõudlus peab olema skaleeritav vastavalt kasutajate ja päringute koguarvule.
Toetatavus (*Supportability*)	▪ Kohandatud muudatused rakenduses peavad olema automaatselt testitavad ja vead tuvastatavad enne, kui klient need avastab. ▪ Rakenduse tarkvara uuendamine peab toimuma *blue-green* juurutusplaani [39] kohaselt, mis minimeerib teenuse maasoleku aega ning vajadusel muudatuse automaatset taastamist.
Juurutamisnõuded	▪ Rakenduse ja andmebaasi puhul tuleb kasutada

(***Implementation requirements***)	avatud lähtekoodiga tarkvara [2.1]. ▪ Kasutada tuleb pidevintegratsiooni (*CI, Continuous Integration*) arendus- ja juurutamismeetodit, et avastada tarkvarauuenduste puhul vead võimalikult varakult ning vähendada käsitsi tehtava töö aega ja seega vigade arvu.

Vastupidiselt FURPS-i abil püstitatavate mittefunktsionaalsete nõuete materjalide vähesusele identiteedi- ja juurdepääsuhalduse lahenduste kohta, leidub selle kohta piisavalt kirjutisi ISO standardite kasutamisest. Järgneb loetelu valitud ISO/IEC dokumente, mille abil on võimalik muuhulgas määratleda süsteemi mittefunktsionaalseid nõudeid [47] .

- ISO/IEC 24760-2:2015, *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements* [41]
- ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements* [42]
- ISO/IEC 27004:2016, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation* [43]
- ISO/IEC 25010:2011, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models* [44]

Mitmed ISO 25010 standardi 8 omadused kattuvad FURPS-i omadustega. ISO/IEC 27001 standard on kõige laialdasemalt levinud infoturbe haldamise karkass maailmas[1] [45] . ISO/IEC 27001:2013 Annex A on lisadokument, mis sisaldab endas juhiseid, mille abil püstitada nõudeid loodavale infosüsteemile. Valik ISO/IEC 27001:2013

1 Eesti infoturbestandard (E-ITS) on kooskõlas ISO 27001-ga, mis on mõeldud asendama varasemat etalonturbe kataloogi Infosüsteemide kolmeastmeline etalonturbe süsteem (ISKE).

Annex A nõudeid, mis oleks loodava identiteedi- ja juurdepääsuhalduse süsteemi mittefunktsionaalsete nõuete jaoks rakendatavad on toodud välja tabelis [Tabel 4].

Tabel 4. ISO/IEC 27001:2013 controls from Annex A IAM jaoks

A.9.1.1	*Access control policy*	Kirjeldab, mis viisil on teostatud juurdepääsuõigused erinevatesse süsteemiosadesse.
A.9.4.3	*Password management system*	Kirjeldab, mis on minimaalsed paroolinõuded ning kuidas hallatakuse nende uuendamist jmt.
A.12.4.1	*Event logging*	Kirjeldab, mis viisil ja mahus korjatakse, talletatakse ning kustutatakse sündmuste logid.
A.13.1.3	*Segregation in networks*	Kirjeldab, kuidas teenused, kasutajad ja süsteemid on teineteisest arvutivõrgu abil eraldatud.
A.18.1.3	*Protection of records*	Kirjeldab, mis krüptoalgoritmide abil on talletatud juurdepääsu logid.

Kui identiteedi- ja juurdepääsuhalduse süsteemi disaini analüüsimisel on järgitud Annex A's kirjeldatud samme (*controls*) ja selle juurutamise järel on võimalik süsteemi kõikide nende sammude abil verifitseerida, siis võib taotleda ISO/IEC 27001 sertifitseerimist, mis tõendab süsteemi usaldusväärsust.

3.4.4 Kasutajaõigused ja -rollid

Käesoleva projekti identiteedi- ja juurdepääsuhalduse süsteemis on olnud peamiselt kasutusel *Attribute Based Access Control* (ABAC) ehk atribuudipõhine juurdepääsu reguleerimine ja vähemal määral *Role Based Access Control* (RBAC) ehk rollipõhine juurdepääsu reguleerimine. Selle peamine põhjus on süsteemide olemasolevate juurutusskriptide konfiguratsioon, kuid ka klientide vajadustega arvestamine.

Igal pilveteenuse süsteemi komponendil on erinev juurdepääsuhalduse võimekus (millest paljudel on võimalik LDAP-i liidestus, kuid kõikidel ka mitte) ning seetõttu on tarvis neid kahte meetodit kombineerida. Parim võimalik lahendus oleks *Next Generation Access Control* (NGAC), mis võimaldaks üksikkasutajatele, rollidele, erinevate osakondade kasutajatele jne määrata ligipääsuõigusi erinevatele ühendustele, süsteemidele ja süsteemi komponentidele ning kaustadele ja failidele. [48]

Projekti IT arhitektuur ei ole NGAC-i juurutamise jaoks veel piisavalt stabiilne ja küps, mis tähendab, et kasutajate ja ligipääsude struktuur on veel liialt dünaamiline ja tarvis on ka *ad hoc* lähenemist. [67]

Võrreldes olemasoleva lahendusega oleks loodava identiteedi- ja juurdepääsuhalduse lahenduse kasutusele võtmisel tarvis muuta juurdepääsuõigusi granulaarsemaks ehk täpsemaks. See tähendab, et ühe kasutajagrupi, näiteks rakenduse X kasutajad A arenduskeskkonnas, saaks jaotada mitmeks osaks: teatud vaadete lugemisõigus, kirjutamisõigus, administreerimise õigused jmt. Samuti saaks ligipääsu seadistada virtuaalmasinate põhiselt ehk igaühele eraldi, mitte kõigile või mitmele korraga terve süsteemi keskkonna või virtuaaltsooni ulatuses. Kasutajagrupid kirjeldatakse iga kliendi kohta erinevalt, vastavalt nende vajadusele ja teenusele, mida pakutakse. Kui on märgata samade kasutajagruppide määramist mitmele erinevale töötajale, siis on võimalik tekitada kasutajagruppide komplekt ehk roll.

Kasutajagrupid ja rollid on otstarbekas algusest peale planeerida taaskasutuse põhimõttel ning seda on parim teha granulaarsete juurdepääsuõiguste abil. [49] Loodud kasutajagruppe ja rolle on kuluefektiivne taaskasutada mitme erineva kliendi jaoks, kui pakutakse sarnase sisuga teenust ning see loob omakorda võimaluse tekitada malle, mille abil juurdepääsuõigusi automatiseeritult tekitada.

3.5 Andmekaitse ja andmeturve

Magistritöö kirjutamise ajahetkel on käsitletav projekt alustamas suveräänse pilve planeerimist, analüüsi ja disaini. See on mõeldud klientidele, kelle puhul on välistatud kasutajate isiklike andmete füüsiline riigipiiride ületamine GDPR-i nõuete kohaselt. [31]

Et regulatsioonidega vastavuses olla, koostatakse regulaarselt klientidele nimekirjad nende ligipääsuõiguste kohta teenusepakkuja süsteemides. Samuti viiakse läbi regulaarselt nii sisene kui klientide ligipääsuõiguste kontroll, mille tulemusel eemaldatakse üleliigsed õigused ja suletakse ebavajalikud või aegunud kontod. See on vajalik eelkõige turvalisuse aspektis, kuid ka auditeerimise tõttu, mida korraldatakse juhuslikus vormis. [29] Varasemalt sai vaid teenusepakkuja seesuguseid puhastamise ja

raporteerimise toiminguid teha, kuid identiteedi- ja juurdepääsuhalduse süsteemi kasutusele võtmisega on seda võimalik ka kliendil teha. [30]

Infosüsteemide arhitektuurne andmeturbe tase määratakse organisatsiooni poolt. IT arhitektuuri andmeturbe saab jaotada kahte osasse.

- Jõudeolekus andmed ehk stabiilsesse säilmällu salvestatud andmete šifreerimine (*data at rest encryption*), mis välistab andmelekke või ründe ohvriks sattunud andmete puhul konfidentsiaalse informatsiooni kuritarvitamise.

- Liikvel olevate andmete ehk arvutivõrgus liikuvate andmete šifreerimine (*data in motion encryption*), mis välistab arvutivõrgu ühenduste pealtkuulamise ründe ohvriks sattunud andmete puhul konfidentsiaalse informatsiooni kuritarvitamise.

Minimaalsed turbenõuded määratakse organisatsiooni üksuse poolt ning alasüsteemid kaitstakse üldise perimeetri tulemüüride abil, kuid rakenduste ja klientidele pakutavate teenuste turbe üksikasjad ja täpsemad väärtused sätestatakse IT arhitektuuri nõukogu [3.4.1] poolt. Sinna alla kuuluvad sümmeetriliste ja asümmeetriliste krüptoalgoritmide ning räsifunktsioonide pikkus bittides, paroolide pikkused ja keerukused jms, mis määravad pilveplatvormi süsteemide ligipääsu turvalisuse ründevektorite eest.

Nende väärtuste haldamist ei pakuta klientidele delegeeritud administreerimisõigustega kaasa, sest teenusepakkuja vastutab ligipääsu turvalisuse eest pakutavale pilveplatvormile. [50] Kliendi otsustada ja vastutusalasse jääb enda loodud infrastruktuuri või teenuste pakkumisega seotud turbenõuete määramine [Joonis 12].

4 Loodava lahenduse kavandamine

Käesoleva peatüki ja selle alapeatükkide eesmärk on kirjeldada püstitatud probleemi [2.2] ning sellele vastava teoreetilise analüüsi [3.4] kohaselt identiteedi- ja juurdepääsuhalduse lahenduse protsesside ja infosüsteemi täiendamise realiseerimise kavandamise ettepanekuid Tietoevry jagatud pilveteenuse keskkonna näitel. Uue süsteemi loomiseks on tarvis planeerimise, analüüsi ja disaini järel sobiva tarkvara testimine, juurutamine, (turva)seadistus, pidevintegratsiooni ja automaattestide arendus, elutsükli halduse välja töötamine ning dokumenteerimine. Samaaegselt uue süsteemi loomisega on tarvis olemasolevate ja uute klientide vanal süsteemil põhineva lahendusega teenindamine. [5]

Autor on analüüsinud ja kirjeldanud probleemi, mis seisneb kvalifitseeritud identiteedi- ja juurdepääsuhalduse töötajate puuduses ja sellega seotud töömahu kasvamises, mis põhjustab teenindusvõimekuse ületamise ja teenindusdefitsiidi tekkimise [2.2], [Joonis 10].

- Teenusepakkuja poolne klientide teenindamine ja kasutajakontode haldamine käsitsi rakenduses A. [2.3]
- Teenusepakkuja poolne juurdepääsuhalduse süsteemi juurutamine uute klientide virtuaaltsoonide ja keskkondade tarvis. [3.1]

Autor on probleemi lahendamiseks välja töötanud sammud, mille täitmisel on võimalik täiendada olemasolevat infosüsteemi, et optimeerida kasutajakontode haldamise ja uute juurdepääsuhalduse süsteemide juurutamise protsessi.

4.1 Äriprotsessi ja osapoolte muudatused

Teenusepakkuja vaatest saaks iga uue kliendi juurdepääsuhalduse süsteemi juurutamist kiirendada automatiseerimise abil ning täiendada kitsaskohti kliendi kasutajate õiguste

haldamisel. Teenusepakkuja sooviks võimaldada kliendil osaleda ja vastutada kliendi enda kasutajate haldust. Klient sooviks pärast ligipääsude tellimist pilveteenust kiiremini kätte saada ja võimaldada enda töötajatel süsteemides tööd alustada, et saaks hakata ärilist väärtust looma [Joonis 1].

Teenusepakkuja äripool peab mõõtma identiteedi- ja juurdepääsuhalduse tegevustele kuluvat ressurssi ja kaardistama uute klientide teenindamise võimekused, et tagada kasutajakogemuse kvaliteet, mida hinnata kasutajate tagasiside abil [Joonis 19]. Tarvis on olla strateegiliselt valmis töömahu kasvamiseks ning arvestama ettevalmistused teenuse hinna sisse, ka juhul, kui vajalike töötundide arvu ei ole võimalik suurendada [3.4.1]. Teenusepakkuja peab investeerima tehnoloogiasse ja töötundidesse, et kiirendada ja täiendada uute klientide juurdepääsusüsteemide juurutamist ning mõõtma selle tulemuslikkust ROI [63] abil. [5]

Jätkustuutliku infosüsteemi arenduse ja halduse protsesside maht on kasvava loomuga [2.2] ja tarkvaraarenduses arvestatakse pidevalt muutuvate nõuete ja funktsionaalsustega, eelkõige agiilses käsitluses. Süsteemide haldamine sisaldab endas serverite ja tarkvara versioonide uuendamist ning eeldab andmemahtude suurenemist ja seega salvestusseadmete lisamist. Järelikult võib pilvandmetöötluse platvormi teenusepakkuja arvestada, et majutatavate töömaht kasvab klientide arvu, klientide kasutajate arvu, klientide töömahu ja klientide klientide töömahu ja kasutajate arvu suurenemisel [Tabel 1], [Joonis 10]. Seesugust kasvu ei ole otstarbekas töötajate arvu suurendamisega hallata, vaid automatiseerida ja võimalusel delegeerida erinevatele osapooltele, k.a. klientidele. [5]

Kõigepealt tuleb eristada protsesse, mida saab automatiseerida ja/või delegeerida ning milliseid ei saa või on selleks ebamõistlikult kulukad. Järgnevalt vaadeldakse lähemalt identiteedi- ja juurdepääsuhalduse olemasolevat töövoogu [Joonis 9] ja tuvastatakse alamprotsessid [Tabel 16], mida on võimalik automatiseerida ja/või delegeerida infosüsteemide juurutamise ja kasutusele võtmise abil. NB! Siin ei ole täpsustatud kliendi töösedelite kasutamise viisid, sest teenusepakkuja vaates ei ole teada ega ka oluline, mis meetodil klient kasutajaõiguste päringuid koostab [3.4.1]. [5]

- Kasutajaõiguste päringu edastamine: kliendi kasutaja poolt tehtav käsitsi toiming, mida on võimalik lihtsustada, kui päring tehakse kliendi enda

süsteemihalduri poole, kes asub organisatsiooni mõttes lähemal ning kelle protsess võib olla kasutajale vähem keerukas, kui teenusepakkujal. [5]

- Päringu kinnitamine: teenusepakkuja kliendihalduri kinnitus ei ole enam vajalik, kui vastav kokkulepe kliendi ja teenusepakkuja vahel on loodud, et kliendi vanemtöötaja (näiteks projektijuht või süsteemihaldur) on selle otsuse eest vastutav. [5]

- Töö vastuvõtmine: olenevalt kliendi haldusprotsessidest võtab kliendi süsteemihaldur uue õiguste lisamise töö vastu. Teenusepakkuja süsteemihaldur valmistab ja teeb kättesaadavaks juurdepääsuhalduse süsteemi ning loob selle tehnilise dokumentatsiooni. Vajadusel osutatakse teenusepakkuja poolset teenusetuge. [5]

- Kasutajakonto ja/või -õiguste muutmine: haldusrakendus B võimaldab graafilises keskkonnas arvutihiire abil kasutajale õigusi lisada kliendile võimaldatud virtuaaltsoonides. [5]

- Sisse logimise info saatmine: haldusrakendus B võimaldab kasutaja loomise ja/või õiguste lisamise järgselt saata kasutajale e-kirja juurdepääsu teabega. [5]

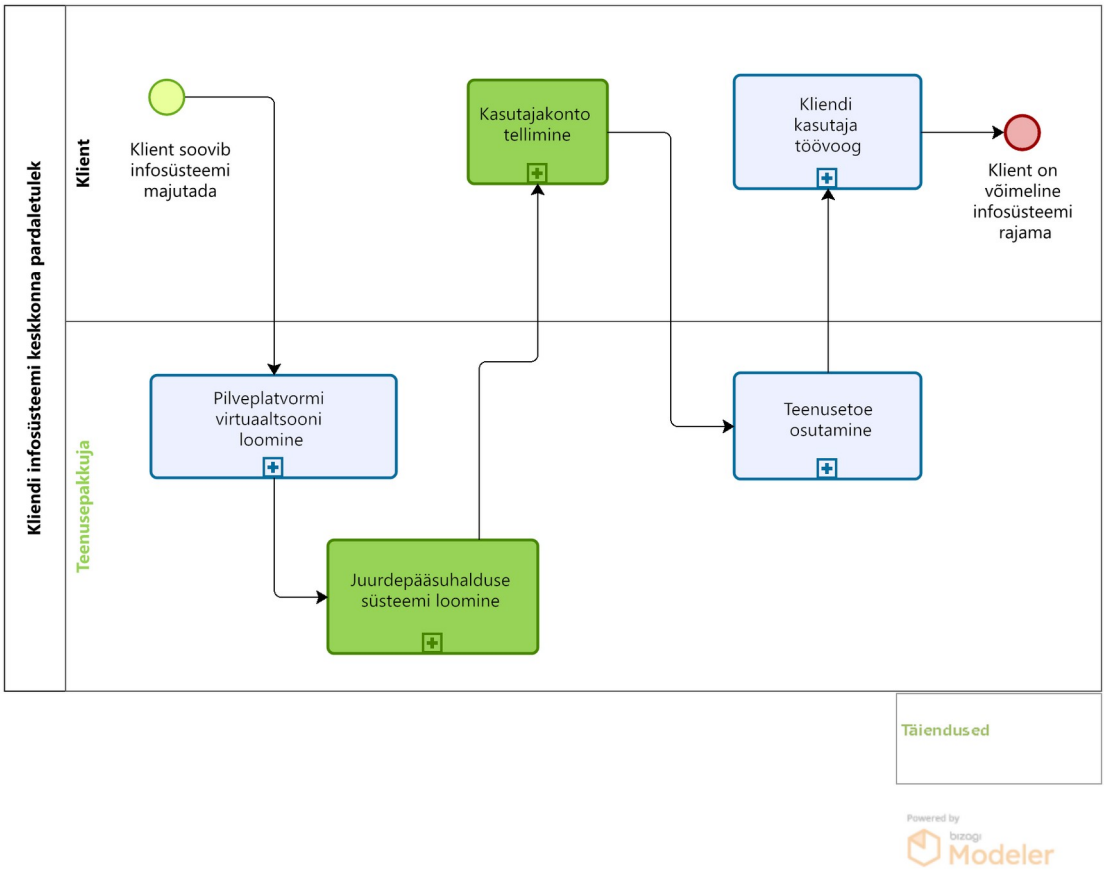
- Kasutajaõiguste kontrollimine ja tagasiside: kliendi kasutaja veendub antud kasutajaõiguste korrektsuses sisse logimisega ja testimisega ning teavitab kliendi süsteemihaldurit kasutajaõiguste õigsusest. [5]

- Töö lõpetamine: kliendi süsteemihaldur on veendunud, et kasutajaõigused on lisatud ja toimivad. [5]

- Päringu lõpetamine: kliendi vanemtöötaja on veendunud ja kinnitanud, et kasutajaõiguste lisamine on lõpule viidud. [5]

Eelneva loetelu peamised täienduste ettepanekud väljenduvad kasutajaõiguste päringute ja haldamise delegeerimises kliendi süsteemihalduritele, kasutades selleks kasutajasõbralikumat ja võimekama funktsionaalsusega tarkvara, mille abil on mugav mainitud toiminguid täide viia [3.4.2]. Seesugune muudatus vähendaks teenusepakkuja süsteemihaldurite töömahtu märgatavalt, sest kasutajaõiguste haldamise töökoormust

vähendatakse iga kliendi arvelt. Kui vastavad kokkulepped [3.4.1] ning tehniliste süsteemide juurutamine ja dokumenteerimine on lõpule viidud, siis on võimalik kõik teenusepakkuja poolt tehtavad klienti puudutavad kasutajaõiguste haldamise toimingud delegeerida kliendile. [5]



Joonis 4. Kliendi infosüsteemi keskkonna pardaletuleku äriprotsessi mudel TO-BE

Kui rakendada pakutud ettepanekud identiteedi- ja juurdepääsuhalduse protsessi muutmiseks, siis muutub peamiselt tellimuste töösedelite haldus, tegelike kasutajaõiguste lisamise tehniline täideviija, kasutajaõiguste haldusrakendus ning informatsiooni vahetamise viis. Joonisel [Joonis 11] on modelleeritud haldussammude erinevused ja täiendused võrreldes AS-IS protsessiga [2.3], mis on osa äriprotsessist [Joonis 4] ja kannab nime „Kasutajakonto tellimine”. Tabelis [Tabel 18] on välja toodud protsesside sisendite ja väljundite erinevused ja täiendused võrreldes AS-IS-iga, kus peamiselt puudub informatsioon võimaliku kliendi sedelisüsteemi kohta, õiguste

lisamine ja selle kinnitamine on delegeeritud kliendi vanemtöötajatele ning sisse logimise info saatmine on automatiseeritud haldusrakenduse abil. Uute rollide vastutusvaldkonnad leiab tabelist [Tabel 19].

4.2 Kasutajalood, vastuvõtukriteeriumid ja prioriseerimine

Selleks, et loodava funktsionaalsuse kasutatavuse tagasiside järgi võimalikult kiiresti kohaneda ja ressurssi liigselt raiskamata juba varajastes faasides muudatusi sisse viia, et kliendi vajadustega ühtlustuda, on tarvis MVP meetodit kasutada [56] , [Joonis 14]. Uute funktsionaalsuste loomisel on abiks kasutajalood ning vastuvõtukriteeriumid, mis on loodud selleks, et teha eesmärgid üheselt mõistetavaks samaaegselt analüütikutele ja tehnilistele töötajatele.

Efektiivsete kasutajalugude defineerimiseks valis autor 3C ja INVEST meetodid [57] , mida kasutatakse samuti käsitletavas projektis SAFe [2.1] karkassi abil. 3C ja INVEST abil verifitseeritakse ja viiakse läbi kvaliteedikontroll juba eksisteerivatele kasutajalugudele ning seejärel püstitatakse vastuvõtukriteeriumid. INVEST tabeli [Tabel 5] puhul väljendatakse iga kasutajaloo kohta eraldi vastavust i*ndependent, negotiable*, *valuable*, *estimable*, *small* ja *testable* hinnangule. Magistritöö loetavuse tõttu on kasutajalood [Tabel 17] järgnevas loetelus esile toodud.

1. Mina teenusepakkujana soovin automatiseeritud identiteedi- ja juurdepääsuhalduse süsteemi juurutamist klientide virtuaaltsoonidesse selleks, et vähendada probleeme, mis võivad käsitsi serverite konfigureerimisel inimvigate ja -viivituste tõttu tekkida.
2. Mina teenusepakkujana soovin automatiseeritud, kiiremat ja optimeeritud kliendi pardaletuleku võimekust selleks, et oleks võimalik müügitehingute arvu suurendada kiirema väärtuspakkumise loomise abil.
3. Mina teenusepakkujana soovin kasutajaõiguste haldamise delegeerida igale kliendile eraldi selleks, et vähendada süsteemihaldurite töökoormust.
4. Mina teenusepakkujana soovin, et iga klient saaks iseenda kasutajate halduse eest vastutada selleks, et vähendada SLA rikkumisi.

5. Mina teenusepakkujana soovin delegeerida kasutajaõiguste päringute kinnitamise või tühistamise kliendi vanemtöötajale selleks, et kliendi kasutajale saaks kiiremini vajalikud ligipääsuõigused määratud.
6. Mina kliendi vanemtöötajana soovin kasutada pilveteenuse juurdepääsu haldusrakenduse iseteenindust delegeeritud administraatori õigustega selleks, et oleks võimalik säästa kuludelt, mis võivad tekkida ajalisest viitest teenusepakkuja ja kliendi vahelise informatsiooni käsitsi vahetamisel.
7. Mina kliendi vanemtöötajana soovin vastutada pilveteenuse juurdepääsu päringute kinnitamise või tühistamise eest selleks, et oleks võimalik kiiremalt ostetud teenust kasutama hakata.
8. Mina kliendi kasutajana soovin kasutada pilveteenuse juurdepääsu haldusrakenduse iseteenindust selleks, et säästa aega parooli taastamisega iseseisvalt.
9. Mina kliendi kasutajana soovin kasutajaliideses vajalikke lahtreid selleks, et redigeerida enda isiklikke andmeid ja seadistust.

Tabel 5. INVEST meetodi rakendamine kasutajalugudele

Kasutajalugu	**Sõltumatu (*Idependent)***	**Täpsustatav (*Negotiable*)**	**Väärtuslik (*Valuable*)**	**Hinnatav (*Estimable*)**	**Väike (*Small*)**	**Testitav (*Testable*)**
1	jah	jah	jah	jah	ei	jah
2	jah	jah	jah	jah	jah	jah
3	ei	jah	jah	jah	ei	jah
4	ei	jah	jah	jah	jah	ei
5	ei	jah	jah	jah	jah	ei
6	ei	jah	jah	ei	ei	ei
7	jah	jah	jah	jah	ei	jah
8	jah	jah	jah	jah	jah	jah
9	jah	jah	jah	jah	jah	jah

INVEST analüüsi tulemusel võib väita, et kuigi kasutajalood 3, 4, 5 ja 6 on paindliku loomuga ja lisavad väärtust, väärivad need tähelepanu, sest nende puhul on tarvis enam keskenduda koostööle teiste osapooltega, neid on tarvis täpsustada ja need ei ole kergesti testitavad.

3C tabel [Tabel 6] on mõeldud kirjeldamaks, kuidas iga kasutajalugu sobib hinnangutega ja on valmis töö alustamiseks.

- C1 kaart (*card*): „kellele?”, „mida?”, „miks?”.
- C2 vestlus (*conversation*): nõuete püstitamine, suhtlemine osapooltega, kokkulepete tegemine.
- C1 kinnitus (*confirmation*): kasutajaloo vastuvõtukriteeriumi sätestamine.

Tabel 6. 3C meetodi rakendamine kasutajalugudele

Kasutajalugu	C1 kaart (*card*)	C2 vestlus (*conversation*)	C1 kinnitus (*confirmation*)
1	jah	ei	jah
2	jah	jah	jah
3	jah	jah	jah
4	jah	jah	ei
5	jah	ei	ei
6	jah	ei	ei
7	jah	ei	jah
8	jah	jah	jah
9	jah	jah	jah

3C analüüsi tulemusel võib väita, et kuigi kasutajalood 5 ja 6 vastavad konkreetselt küsimustele „kellele?”, „mida?” ja „miks?”, väärivad need tähelepanu, sest nende puhul on tarvis enam keskenduda nõuete püstitamisele ja nendele vastavuse selgitamisele ning erinevate klientidega läbirääkimistele ja ühtlustamisele.

Vastuvõtukriteeriumid on sätestatud iga kasutajaloo kohta eraldi tabelis [Tabel 7] kasutades *given-when-then* [58] metoodit.

Tabel 7. Kasutajalugude vastuvõtukriteeriumid

Kasutajalugu	**Vastuvõtukriteeriumid (a*cceptance criteria*)**
1	▪ Kui ma kasutan automatiseeritud juurutusskripte identiteedi- ja juurdepääsuhalduse süsteemi loomiseks mallide abil, siis täidetakse sisendandmete põhjal vastavad parameetrid ning süsteemi toimivust testitakse integratsioonitestide abil. ▪ Kui ma olen automatiseeritud juurutusskripte identiteedi- ja juurdepääsuhalduse süsteemi loomiseks mõeldud mallis teinud vea, siis annab süsteem sellest teada ja katkestab juurutamise protsessi. ▪ Kui ma kasutan automatiseeritud kliendi infosüsteemi pardaletulekut, siis toimub selle täideviimine deklaratiivsel viisil ja soovitav lõpptulemus kirjeldatav konfiguratsioonifailidena.
2	▪ Kui vastav IT taristu on loodud, siis on uue kliendi nime ja süsteemide keskkondade nimetuste abil võimalik paigaldada ja seadistada esmane IAM lahenduse versioon ning võimaldada see kliendile kasutamiseks tundide jooksul. ▪ Kui kliendi pardaletuleku protsess on optimeeritud, siis saab uutele potentsiaalsetele klientidele teha kättesaadavaks praktilisi esitlusi töötava süsteemiga ja lasta ka seda proovida (*look and feel*).
3	▪ Kui kliendi vanemtöötajal on piiratud õigused hallata kasutajaõigusi, siis on ta võimeline enda kasutatavatesse süsteemidesse ligipääsemiseks ise kasutajakontosi looma ja nendele juurdepääsuõiguseid andma. ▪ Kui kasutajaõiguste haldus on delegeeritud igale kliendile, siis väheneb teenusepakkuja süsteemihaldurite töömaht selle arvelt

	ja on võimalik teisi tööülesandeid teha. ▪ Kui kliendi vanemtöötaja logib IAM süsteemi sisse, siis on tal võimalik hallata kasutajaõiguseid infosüsteemide keskkondades, mis on temale teenusepakkuja poolt võimaldatud.
4	▪ Kui klient vastutab iseenda kasutajate halduse eest, siis ei ole teenusepakkujal vaja jälgida iga ligipääsuõiguste päringu SLA-d ja väheneb risk trahvisummade määramise risk. ▪ Kui kliendid vastutavad enda kasutajate ligipääsuõiguste eest, siis väheneb teenusepakkuja poolsete töösedelite menetlemise arv ja võidetakse aja poolest.
5	▪ Kui klient saab kinnitada või tühistada enda kasutajate ligipääsuõiguste päringuid, siis on vähem teenusepakkuja ja kliendi vahelist informatsiooni vahetamist ja kliendi kasutajad saavad ligipääsuõigused kiiremini kätte. ▪ Kui klient saab kinnitada või tühistada enda kasutajate ligipääsuõiguste päringuid, siis väheneb teenusepakkuja poolne risk kasutajaõiguste väärkasutamise suhtes.
6	▪ Kui kliendi kasutajate ligipääsuõigusi haldavad kliendi vanemtöötajad, siis on informatsiooni vahetamine potentsiaalselt kiirem ja klient saab kiirema ligipääsu määramise abil kiiremini väärtust looma hakata. ▪ Kui kliendi kasutajate ligipääsuõigusi haldavad kliendi vanemtöötajad, siis on ligipääsuõiguste eemaldamine efektiivsem ja turvalisem. ▪ Kui kliendi vanemtöötaja haldab kasutajaõigusi, siis on tal selleks vastavad õigused ja dokumentatsioon kättesaadavad.
7	▪ Kui kliendi vanemtöötaja saab ise vastutada juurdepääsu päringute kinnitamise või tühistamise eest, siis ei ole vaja

	teenusepakkuja poole selle jaoks eraldi pöörduda ja juurdepääsu tehnilist teostust saab alustada varem. ▪ Kui kliendi vanemtöötaja saab ise vastutada juurdepääsu päringute kinnitamise või tühistamise eest, siis on võimalik efektiivsemalt tühistada ligipääsu ja on võimalik vältida sellega seonduvaid turvariske.
8	▪ Kui kliendi kasutaja unustab enda ligipääsu parooli, siis ta saab seda iseteeninduse abil taastada ja iseseisvalt teenust edasi kasutada. ▪ Kui luuakse uus kasutajakonto, siis saab parooli taastamise abil pardaletulekut osaliselt kliendi kasutajale delegeerida ja halduskoormust veelgi vähendada.
9	▪ Kui kliendi kasutaja isiklikud andmed muutuvad, siis on seda võimalik iseteeninduse abil teha, mis säästab aega, kui pole vaja sellega seotud päringuid teha. ▪ Kui kliendi kasutajal on vaja seadistusi muuta, siis on seda võimalik iseteeninduse abil teha, mis säästab aega, kui pole vaja sellega seotud päringuid teha. ▪ Kui klient soovib serveritesse autentimist turvalisemalt läbi viia, siis lisaks parooli abil autentimisele, saab ta RSA võtmepaariga autentida ja ise lisada enda avaliku võtme, mis tehakse serveritele automaatselt kättesaadavaks.

Inkrementaalse arenduse põhimõtete järgi ja arendustööde tegemise võimekuse tõttu ei ole võimalik kõiki püstitatud kasutajalugusi koheselt töösse võtta. Seetõttu tuleb viia läbi prioriseerimine, et selgitada välja, missugused kasutajalood ja funktsionaalsused võivad tuua kliendile ja seega teenusepakkujale enim väärtust. Prioriseerimiseks on valitud MoSCoW ja Kano meetodid, mis täiendavad teineteist, väljendudes vastavalt

toote/teenuse ja turu vaadetes [65] . MoSCoW abil prioriseerimise tabelis [Tabel 8] on välja toodud kasutajalood ja sulgudes on selguse mõttes kasutajalugude nummerdus.

Tabel 8. Kasutajalugude peamise funktsionaalsuse prioriseerimine MoSCoW abil

Peab olema (Must have)	**Peaks olema (*Should have*)**	**Võiks olla (Could have)**	**Ei pea olema (Won't have)**
Deklaratiivne automatiseeritud pardaletulek (1)	Kliendi töövoo optimeerimine (6)	Ligipääsuõiguste kinnitamise delegeerimine (7)	-
Kasutajaõiguste haldamise delegeerimine (3)	Kiirem ligipääs kliendile (5)	Identiteedi redigeerimise iseteenindus (9)	-
Kliendi vastutuse suurendamine (4)	Kiirem tarne ja müük (2)	Parooli taastamise iseteenindus (8)	-

Kano ja MoSCoW mudelid ei ole omavahel asendatavad: MoSCoW mudeli "*must be*" ja Kano mudeli "*must be*" ei ole samad. MoSCoW kuulub tooteomanikule ja sellel on tootepõhine perspektiiv. Kano põhineb tootehalduse, müügi, konkurentsianalüüsi jms sisendil, millel on turupõhine perspektiiv. Nende kahe meetodi kombineerimine võib olla agiilsete meeskondade jaoks väga väärtuslik. Pakkudes "*must-be*", "atraktiivsete" ja "ühemõõtmeliste" featuuride kombinatsiooni koos "kohustuslike" featuuridega vastavalt MoSCoW-le, saab suurendada tõenäosust, et toode või teenus saab olema kliendisõbralik ja turuvalmis. [65]

Joonis 5. Kasutajalugude peamise funktsionaalsuse prioriseerimine Kano mudeli abil

Kasutajalugude töösse võtmise prioriseerimisel arvestatakse äristrateegia eesmärkidega [2.3.3], [Joonis 18], [Joonis 19], mis võimaldaks teenuse võimalikult kiire ja kvaliteetse turule toomise, teenides klientide ja teenusepakkuja ärilisi huve ja arvestades ennetavalt tõenäoliste muudatustega.

4.3 Tehnilise lahenduse juurutamise kavandamine

Autori roll antud probleemi tehnilisel lahendamisel on kavandada identiteedi- ja juurdepääsuhalduse süsteemi MVP SaaS lahendus, mida kliendile ärilise väärtusena pakkuda. Esialgne versioon peab võimaldama tarkvarakomponentide omavahelisel integreerimisel kasutada kliendil hallatud teenusena funktsionaalsust, mis on kirjeldatud punktides [3.4.2] ja [4.1].

Käesoleva probleemi tehnilise lahenduse puhul on tegemist olemasoleva (kolmandate osapoolte loodud[1] ja osaliselt IT arhitektuuri nõukogu [3.4.1] poolt valitud) identiteedi- ja juurdepääsuhalduse tarkvara ning sõltuva tarkvara juurutamise- ja

1 Identiteedi- ja juurdepääsuhalduse lahenduse täiendamise tarkvarakomponentide valik ja nimetused [3.4.1] ei ole avaldatud.

konfigureerimisega. Identiteedi- ja juurdepääsuhalduse tehnilise lahenduse juurutamise protsess on ette nähtud korratavana, mis tähendab, et iga kliendi jaoks paigaldatakse samasugused süsteemi komponendid. Erinevus klientide süsteemide vahel on komponentide range arvutivõrkude põhine eraldatus virtuaaltsoonidesse ja kliendi ning kliendi süsteemide keskkondade nimetustel [4.3.1] põhinevate muutujate väärtuste deklaratiivne kasutus konfiguratsioonifailides.

Järgnevalt kirjeldatakse loodava identiteedi- ja juurdepääsuhalduse lahenduse süsteemi olulisimaid komponente ja nende omavahelisi seoseid, mis erinevad olemasoleva lahenduse poolest. Olemasoleva juurdepääsuhalduse lahenduse süsteemi funktsionaalsus peab täies mahus säilima, vähemalt üleminekuperioodi vältel. [2.4], [Joonis 16] Riistvara, andmekeskused, arvutivõrgu topoloogia, andmesalvestustehnoloogiad, hüperviisorid jmt IaaS ülalhoiuks vajalik madalama taseme IT taristu arhitektuur, mille eest autor ei vastuta [3.4.1], ei tule käsitluse alla, välja arvatud, kui sellel on otsene seos ja/või põhjus juurdepääsuhalduse lahenduse süsteemi toimimisel.

Loodav süsteem põhineb esi- ja tagarakenduste (*front-end and back-end*) arhitektuuril, mille puhul autentimisteenuse tagarakenduse server (serveriklaster) on andmete hoiundamiseks ja veebiliidesega esirakenduse server (serveriklaster) on nende andmete haldamiseks ette nähtud, mis omakorda duplitseerib need andmed eraldiseisvasse tagarakenduse andmebaasiserverisse (serveriklastrisse) ja on ühendatud e-posti rakendusserveriga (serveriklaster), mis võimaldab teavitusi ja iseteeninduslikku parooli taastamist. Kõikide serveriklastrite ette on seadistatud koormusjaotur, et suurendada käideldavust serveri rikete puhul.

Klientrakendused, mis esirakenduse veebiserveri teenust kasutavad, võimaldavad lisaks LDAP-i protokollile veel SAML ja OIDC autentimis- ja autoriseerimisühendusi jmt. Klientide kasutajatele on iseteenindus avatud esirakenduse veebiserverist turvalise teenuselüüsi abil [Joonis 17]. Rakendusserverite juurutamine toimub parametriseeritud mallide (*template*) ja automatiseeritud skriptide käsitsi käivitamise abil. Skriptide abil on võimalik paigaldada ja seadistada iga serveripaari jaoks tegevused, mida kirjeldati loetelus punktis [2.4], lisategevused seoses uute komponentidega ja lisaks automatiseerida eelnevaid käsitsi tehtavaid toiminguid [3.1].

- Kasutajate andmete importimine ja automaatne sünkroniseerimine autentimisteenuse tagasüsteemist esisüsteemi ja selle vastavasse andmebaasi.
- E-posti saatmise seadistus.
- Andmebaaside seadistamine ja täitmine tabelite ning kirjetega.
- Serveripaaride arvutivõrkude ühenduste turvamine TLS-i abil. [3.1]
- Serveripaaride andmebaasides sisalduvate kasutajaandmete automaatne sünkroniseerimise omavahel. [3.1]
- Iganenud ja vähemturvaliste krüptoalgoritmide keelamine. [3.1]
- Minimaalsete paroolinõuete määramine. [3.1]
- Virtualiseeritud koormusjaoturi (Load Balancer) paigaldamine ja seadistamine selleks, et klientrakendused oleksid võimelised kasutama kõrgkäideldavat serveri teenust, kui on võimalik sisestada vaid 1 IP aadress või serveri nimi, mitte mõlemad. [3.1]
- Juurutatud lahenduse automaattestide abil kontrollimine. [4.3.2]

Nende etappidega on esmane identiteedi- ja juurdepääsuhalduse süsteemi komponentide paigaldus ja seadistus lõpetatud, eeldades, et väliste arvutivõrkude ühendused on eelnevalt avatud ja kontrollitud.

4.3.1 Kasutajaõigused ja -rollid

Iga majutatava kliendi infosüsteem sisaldab endas erinevaid teenuseid, mida teenusepakkuja osutab. Selle põhjal luuakse dünaamilised tabelid, milles defineeritakse missugustele teenustele saavad kliendi delegeeritud õigustega administraatorid hallata ligipääsu kliendi enda kasutajatele. Kliendid struktureerivad ligipääsu näiteks osakondade, projektide, kompetentside ja süsteemide järgi.

Näites [Tabel 11] kujutatakse stsenaariumi, milles teenusepakkuja osutab kliendile veebirakenduse SaaS teenust, mille seire toimub monitooring M abil ning nende haldus toimub hüppeserver H kaudu. Rakenduse R ja hüppeserveri H puhul on lubatud õiguste

delegeerimine vaid arenduskeskkonnale ja testimiskeskkonnale, kuid mitte toodangukeskkonnale, sest lepingu kohaselt vastutab teenusepakkuja toodangukeskkonna toimivuse eest. Monitooring M andmete lugemisõiguse delegeerimine on kõikides keskkondades lubatud, kaasa arvatud toodangukeskkonas, sest kliendile on oluline omada ligipääsu enda toodangukeskkonda puudutavale meetrikale igal ajahetkel.

Tabel 9. Delegeeritud kasutajaõigused klientide virtuaaltsoonide keskkondade põhjal

Teenus	**Kasutajagrupp**	**Arenduskeskkond (*development environment*)**	**Testkeskkond (*test environment*)**	**Toodangukeskkond (*production environment*)**
Monitooring M SaaS	Andmete lugemisõigus	Jah	Jah	Jah
	Andmete lugemis- ja kirjutamisõigus	Jah	Jah	Ei
Rakendus R SaaS	Konfiguratsiooni lugemis- ja kirjutamisõigus	Jah	Jah	Ei
Hüppeserver H SaaS	Tavakasutaja õigustes kaughaldus	Jah	Jah	Ei
	Administraatori õigustes kaughaldus	Jah	Jah	Ei

Atribuudipõhine juurdepääsu reguleerimine võimaldab tekitada kasutajagruppe, millesse kuuluvad kasutajad saavad ligipääsu teatud virtuaaltsooni keskkonna süsteemi täpse seadistusega. Olenevalt süsteemi (näiteks virtuaalserveri) võimekusest saab konfigureerida näiteks lugemis- ja kirjutamisõiguse teatud kaustale, failile või vaatele ja seejärel vastendada (*mapping*) selle kasutajagrupiga ligipääsu süsteemis. Järgneva näite [Tabel 9] põhjal pakutavatest teenustest, mille juurdepääsu delegeeritud administaatori õigustega klient saab kliendi enda kasutajatele määrata [Tabel 10].

Tabel 10. ABAC näited klientide virtuaaltsoonide keskkondade põhjal

Kasutajagrupp	**Kasutaja**	**Arenduskeskkond (*development environment*)**	**Testkeskkond (*test environment*)**	**Toodangu-keskkond (*production environment*)**
Monitooring M andmete lugemisõigus	Veebiarendaja1	Jah	Ei	Ei
	Vanemarendaja	Jah	Jah	Jah
Rakendus R konfiguratsiooni lugemis- ja kirjutamisõigus	Veebiarendaja1	Jah	Ei	Ei
	Vanemarendaja	Jah	Jah	Ei
Hüppeserver H tavaõigustes kaughaldus	Veebiarendaja1	Jah	Ei	Ei
	Vanemarendaja	Jah	Jah	Ei
Hüppeserver H administraatori õigustes kaughaldus	Veebiarendaja1	Ei	Ei	Ei
	Vanemarendaja	Jah	Ei	Ei

Rollipõhine juurdepääsu reguleerimine võimaldab tekitada kasutajagruppidest omakorda kasutajagruppide komplekte, millesse kuuluvad kasutajad saavad ligipääsu määratud virtuaaltsooni keskkondade süsteemide kombinatsioonidele. Olenevalt süsteemide (näiteks virtuaalserverite) võimekustest saab konfigureerida näiteks lugemis- ja kirjutamisõiguse teatud kaustadele, failidele või vaadetele ja seejärel vastendada (*mapping*) selle kasutajarolliga ligipääsu süsteemis. Kasutajaroll võib olla näiteks algtasemel tarkvaraarendaja, kellel on vaid arenduskeskkonna teatud süsteemi osadesse lugemisõigus ja mõnesse ka kirjutamisõigus.

Tabel 11. RBAC näited klientide virtuaaltsoonide keskkondade põhjal

Kasutaja	**Roll**	**Kasutajagrupp**
Veebiarendaja2	Rakendus R veebiarendaja	▪ Monitooring M andmete lugemisõigus arenduskeskkonnas ▪ Rakendus R konfiguratsiooni lugemis- ja kirjutamisõigus arenduskeskkonnas ▪ Hüppeserver H tavaõigustes kaughaldus arenduskeskkonnas
Domeeni administraator	Rakendus R lahenduse süsteemiadministraator	▪ Monitooring M andmete lugemisõigus arenduskeskkonnas, testkeskkonnas ja toodangukeskkonnas ▪ Rakendus R konfiguratsiooni lugemis- ja kirjutamisõigus arenduskeskkonnas, testkeskkonnas ja toodangukeskkonnas ▪ Hüppeserver H administraatori õigustes kaughaldus arenduskeskkonnas ja testkeskkonnas

RBAC lähenemisest on kasu, kui näiteks meeskonnaga liitub uus töötaja (veebiarendaja2), kellel on vaja samasuguseid õiguseid, nagu kolleegidel meeskonnas, kes sama süsteemiga töötavad või süsteemiadministraatoritel, kellele on tarvis mitmed ligipääsud erinevatesse keskkondadesse ja rakendustesse korraga anda.

4.3.2 Automaattestid ja tarneahelad

Identiteedi- ja juurdepääsuhalduse süsteemi juurutamisskriptid loovad funktsionaalsuse, mis on kirjeldatud funktsionaalsete nõuete [3.4.2] ja kasutajalugude [4.2] punktides ning vastuvõtukriteeriumitega tabelis [Tabel 7]. Need funktsionaalsused on mõeldud kliendile väärtuse loomiseks ning nende toimivuse käsitsi kontrollimine pärast identiteedi- ja juurdepääsuhalduse süsteemi tarkvara uuendamist või juurutamist ei ole efektiivne. Seetõttu on vajalik automaattestide arendamine, mille loomisega tuleb süsteemi integreerimise testimise algusest peale tegeleda. See vähendab süsteemis tekkivate tõrgete tõenäosust, kui esineb kolmandate osapoolte tarkvaraliste sõltuvuste, tarkvarauuenduste, konfiguratsiooni ning funktsionaalsuste lisamise ja/või muutumist.

Selleks, et olla ennetavalt valmis eelnevalt mainitud muudatustega kohanemiseks enne, kui uue versiooni tarne virtuaaltsoonide keskkondadesse toimub on DevOps [2.1] meetodile kohaselt tarvis juurutada tarneahel (*pipeline*), mis võimaldab automatiseeritud integratsioonitestide ja läbivtestimise (*end-to-end testing*) abil veenduda, et just sellises keskkonnas ja sellise konfiguratsiooniga on lahendus võimeline lubatud funktsionaalsused tekitama. Tarneahelat võib käivitada kokku lepitud intervallidega kas automatiseeritult või automaatselt. Tarneahela tüübid on järgnevad.

- Pidevintegratsioon ehk *continuous integration* (CI), mis võimaldab tarkvara- või süsteemiintegratsiooni automatiseeritud ülesehituse (*build*) abil käsitsi tegemisega võrreldes kiiresti leida üles veakohad ja saada uuest funktsionaalsusest või versiooniuuendusest arusaam, mille abil olla valmis agiilselt muutuvate nõuete jaoks. [59]

- Pidevvalmidus ehk *continuous delivery* (CD), mis võimaldab pidevintegratsiooni õnnestumise puhul valmistada tarkvara- või süsteemiintegratsioon automatiseeritult ette tarneks elutsükli keskkonda (et olla näiteks valmis seda kiiresti kliendile kättesaadavaks tegema). [59]

- Pidevtarne ehk *continuous deployment* (CD), mis võimaldab pidevvalmiduse õnnestumise puhul teha automatiseeritud tarkvara- või süsteemiintegratsiooni tarne ehk juurutamine elutsükli keskkonda (et tarnida kokku lepitud ajal näiteks

kliendile). Otstarbekas on pidevtarnet kasutada vaid arendus- ja testkeskkondades, aga mitte toodangukeskkonnas. [59]

Käesoleva identiteedi- ja juurdepääsuhalduse süsteemi lahenduse puhul on kavas juurutada pidevintegratsioon MVP raames ning ennetavalt arvestada tulevaste arendustega pidevvalmiduse ja pidevtarne loomiseks. Kuna pidevintegratsioon sisaldab endas identiteedi- ja juurdepääsuhalduse süsteemi funktsionaalsuste valideerimiseks automaatteste, siis võib väita, et lahendus, mis kliendini jõuab on sama kvaliteetne kui on süsteeminõuete ja testide kvaliteet. Sellega vähendatakse käsitsi tehtavate toimingute [3.1] puhul tekkivaid vigu uute süsteemide juurutamisel uute klientide ja nende keskkondade jaoks ning vähendatakse tekkivat *overhead* töökoormuse kasvu ja seega säästetakse kuludelt. „Juurdepääsuhalduse süsteemi loomine” alamprotsess on nähtav joonisel [Joonis 4].

5 Tulemused

Käesoleva peatüki eesmärk on analüüsida ja hinnata, kuidas kavandatav infosüsteem sobib püstitatud probleemi ja nõuete lahendamiseks. Uue lahenduse arendustööd tekitavad ajutiselt kõrgema tööhõive ning vaja on kaasata ka teisi meeskonnaliikmeid, sest olemasolevaid kliente on tarvis jätkuvalt teenindada olemasoleva süsteemi abil ning uute juurutamiste puhul teha lisaks automatiseeritud skriptide tööle ka vajalikud käsitsi toimingud [3.1].

Pärast identiteedi- ja juurdepääsuhalduse protsessi muudatusi ning uue süsteemi juurutusskriptide loomist ja kasutusele võtmist väheneb teenusepakkuja töötajate töömaht klientide kasutajate halduse ning uute keskkondade süsteemide juurutamiste arvelt, sest kasutajate haldus on delegeeritud klientidele ja süsteemide juurutamine on optimeeritud. Mõõdikud ja KPI-d, mida optimeeritakse on järgnevad.

- Klientide delegeeritud administraatorid näevad vaid kliendi enda spetsiifilise virtuaaltsooniga seotud keskkondi ja kasutajagruppe, mis välistab valedesse keskkondadesse õiguste lisamise ja sellega seotud lisakulude tekkimise. [5]

- Teenusepakkuja ei vastuta enam klientide kasutajaõiguste lisamise eest ning seega ei ole enam võimalik sellega seonduvat SLA-d rikkuda. [5]

- Kliendi vanemtöötajate ja kliendi kasutajate vahelised seosed on nende endi vastutada ja protsessid on potentsiaalselt ka optimaalsemad kui teenusepakkuja ja kliendi vahelised seosed. Informatsiooni vahetamine on sujuvam, mis tingib sellega seonduvate lisakulude vähenemise. [5]

- Kasutajaõiguste süsteemi komponentide haldus on keskselt automatiseeritud ja testitud pidevintegratsiooni tarneahelas, mis vähendab käsitsi tehtavate toimingute ajakulu ja vigadega seonduvaid lisakulusi. [5]

- Sujuv, automatiseeritud, testitud ja kasutajasõbralik identiteedi- ja juurdepääsuhalduse keskkond on uutele klientidele atraktiivne funktsionaalsus ning võimaldab pilveteenuse müügitööd efektiivsemaks muuta. [5]

- Teenusepakkuja süsteemihaldurite töömaht väheneb ja seda on võimalik ennetavamalt planeerida, kui tegeletakse peamiselt klienditoe osutamisega. [5]

Edaspidiselt saavad peamised identiteedi- ja juurdepääsuhaldusega seotud toimingud olema toodangus olevate süsteemide ülalhoid ning teenusetugi kliendi süsteemihalduritele. [5]

5.1 Kvantitatiivsed näitajad

Probleemi püstituses punktis [2.2] on väljendatud tööhõive [Tabel 1] ja [Joonis 10], mis ületab teenusepakkuja teenindusvõimekuse juhul, kui klientide ligipääsusüsteeme tuleb juurde luua, klientide kasutajate kontode haldamise töömaht suureneb kliendi algatusel või teenusepakkuja identiteedi- ja juurdepääsuhalduse töötajad on teiste kõrgema prioriteediga kohustustega hõivatud.

Pärast identiteedi- ja juurdepääsuhalduse protsesside ja infosüsteemi juurutamist, kui arenduskulud on minimaalsed ja alles on jäänud peamiselt halduskulud ja tugiteenuse kulud väheneb autori hinnangul tööhõive kuni 75% ulatuses, mis on samas ettepanek strateegiliseks eesmärgiks (*goal*).

Töötajate täistööajast juurdepääsuhalduse tegevustele kulunud aritmeetiline keskmine aeg kliendi kohta on välja arvutatud töötundide arvestuse raportite ajaloo abil lahenduse prototüübi kasutamise perioodil 3 kuu vältel ja näidatud tabelis [Tabel 12] ja joonisel [Joonis 13]. Kumuleeritud FTE-de arv kahe töötaja 5 kliendi arvestuses oli 1.7[1] [Tabel 1], mis väheneb uue hinnangulise tööaja 0.45[2] tõttu 1.25[3] võrra, mis on võrdeline 200[4] säästetava töötunniga kalendrikuus. Eesti keskmise DevOps inseneri netokuupalga

1 $0.1+0.2+0.1+0.15+0.05+0.2+0.4+0.1+0.3+0.1=1.7$
2 $0.03+0.05+0.03+0.04+0.01+0.05+0.1+0.03+0.08+0.03=0.45$
3 $1.7-0.43=1.25$
4 $160 \cdot 1.25=200$

2706[1] [61] , mille tööandja kulu kokku on 4694[2] [62] juures on 200 töötundi täiskohaga töötaja ettevõttele säästnud 5867[3] € ulatuses kuus ja 70 410[4] € aastas.

Tabel 12. Kvalifitseeritud IAM töötajate FTE jaotus klientide vahel TO-BE

	Klient 1	**Klient 2**	**Klient 3**	**Klient 4**	**Klient 5**	**Kokku**
Töötaja 1 FTE	0.03	0.05	0.03	0.04	0.01	**0.16**
Töötaja 2 FTE	0.05	0.1	0.03	0.08	0.03	**0.29**
Kokku	**0.08**	**0.15**	**0.06**	**0.12**	**0.04**	**0.45**

Kui kasutajate loomise ja juurdepääsuõiguste loomise tehniline protseduur on klientidele delegeeritud, siis otsene tööaeg teenusepakkuja vaatest puudub. Edaspidiselt kulub sellega seotud teenusetoele osutamisele suurusjärgus kümnendik eelnevalt kulunud tööajast.

Virtuaaltsooni ligipääsuhalduse süsteemi pardaletulek esialgse MVP lahenduse prototüübi testimisel oli keskmiselt tund aega, kui välja arvata arvutivõrkude ja muu taristu ettevalmistused, mis on enamjaolt ühekordsed. See on olemasoleva lahendusega võrreldes (keskmiselt kuni 2 nädalat [3.2]) hinnanguliselt 80 korda kiirem. Loodava pardaletuleku automatiseeritud protsessi ei ole täpsemini analüüsitud, sest see on harvemini tehtav toiming ja selle testimine ei loo hetkel olulist väärtust.

5.2 Lahenduse kavandi tagasiside ja ettepanekud

Autor küsitles ja koostas koondatud tulemustest DAKI meetodi abil tabeli [Tabel 13], mida aitas täita DevOps team [2.3.2] meeskond, milles ta on ise liige. DAKI meetodi abil on võimalik planeeritud ja/või tehtud tööd hinnata ning seda kasutada sisendiks, et prioriseerida edaspidiseid tegevusi.

1 $(3874+1539)/2=2706$

2 $2706+583.75+48.44+60.56+24.22+999.16\approx4694$

3 $4694\div160\cdot200\approx5867$

4 $5867\cdot12=70410$

Tabel 13. DAKI tagasivaatav (*retrospective*) analüüs

Loobu (*Drop*)	**Lisa (*Add*)**
▪ Suurte kasutajalugude tööde üle kandmine järgmistesse arenduse iteratsioonidesse (*sprint*'idesse). ▪ Keeruliste lahenduste tervikuna käsitlemine (vajalik tükeldamine).	▪ Suurte kasutajalugude tükeldamine. ▪ Organisatsioonis kasutatavate sarnaste lahenduste analüüs. ▪ Täpsem kliendile pakutava teenuse väärusvoo kirjeldus.
Säilita (*Keep*)	**Täienda (*Improve*)**
▪ Strateegia ja kliendi vajadustest lähtumine. ▪ Analüüsimeetodite kombineerimine ja võrdlemine. ▪ Ettevõtte- ja IT arhitektuuri seostamine. ▪ Süsteemi nõuete defineerimine ja skoobi määramine.	▪ Kaasata enam kliendi kasutajaid ja insenere planeerimise faasides. ▪ Täpsem IAM tegevusteks kuluva aja mõõtmine ja dokumenteerimine. ▪ Kasutajalugude vastuvõtukriteeriumite täpsustamine.

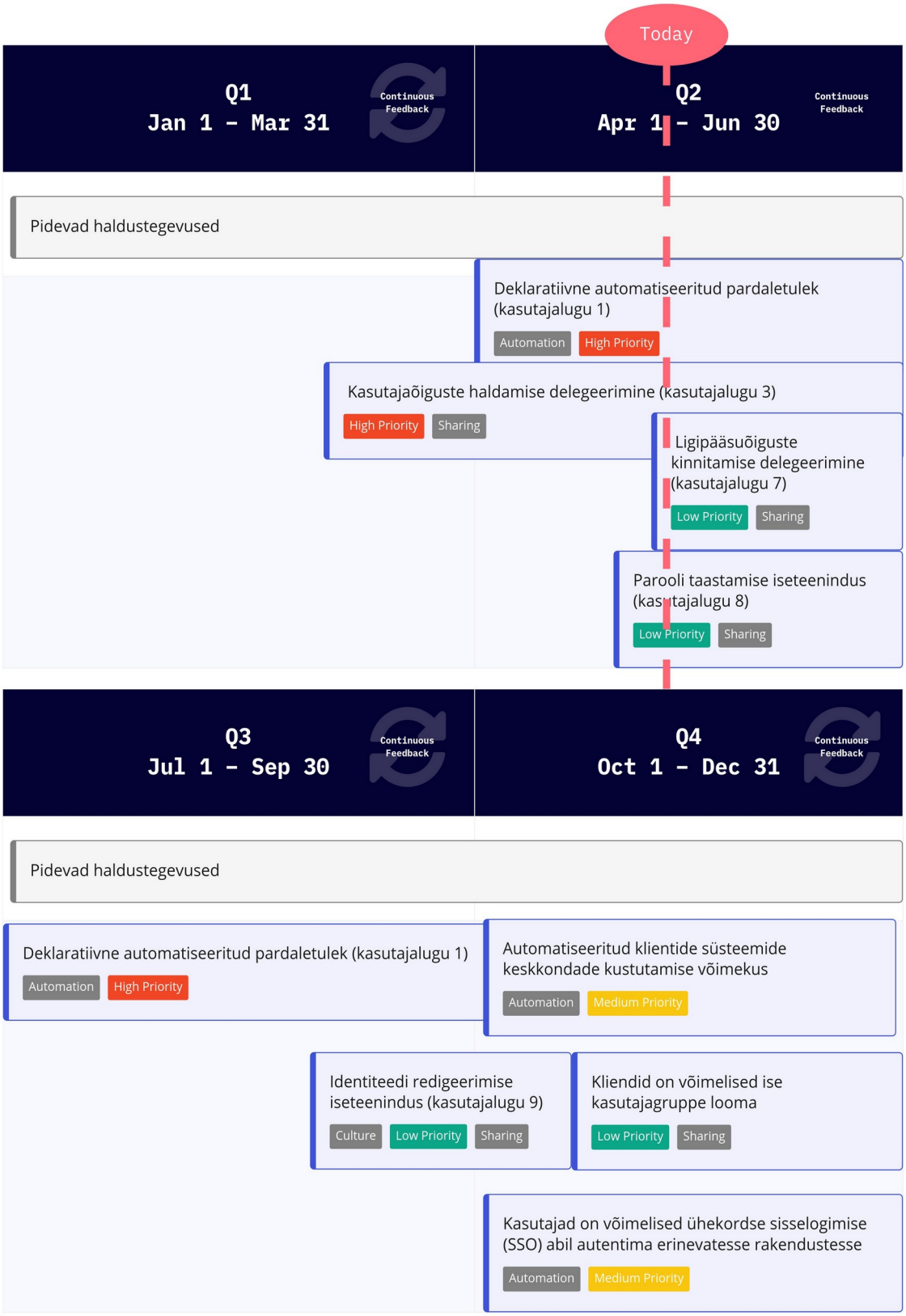
Klientidele koostatud küsimustiku tulemused on kajastatud tabelis [Tabel 20]. Küsimused 5 – 10 vastused on kvalitatiivsed ning nende põhjal võib järeldada, et ligipääsude haldus on olemasoleva lahenduse puhul aeganõudev ja tülikas, tugiteenuste kvaliteet ja informatsioon on vähesed ning eelistatud oleks ligipääsude haldust korraldada kliendi poolel. Samas ollakse rahul pilveteenuse meeskonna suhtumisega, kasutatavate tehnoloogiatega jmt, kuid vastused ei ole vastanute poolt koondunud, vaid pigem hajutatud.

Autor on analüüsinud ja kavandanud lahenduse, mis aitaks mainitud probleeme lahendada, mida on ka kliendid märganud. Kui lahendus realiseerida, siis oleks võimalik sama küsitluse abil hinnata lahenduse tulemuslikkust klientide kasutajate rahulolu ja

kasutajakogemuse vaatest. Autor on teinud ja kavatseb jätkata magistritöö põhjal ettepanekute tegemist muudatusteks organisatsiooni projekti protsessides ja infosüsteemides, mis on seotud juurdepääsuhaldusega, et olukorda parendada [5.3].

5.3 Potentsiaalne arendusplaan

Autor on välja pakkunud käesoleva 2022. aasta tegevuskava, mis hõlmab käimasolevaid ja magistritöös püstitatud eesmärgi saavutamiseks vajalikke infosüsteemidega seotud samme. Teekaart (*roadmap*) [Joonis 6] on visualisatsioon tehtud ja planeeritavatest töödest aasta kvartalite lõikes, mis loovad arusaadava ülevaate epikute ja/või kasutajalugude abil nii tehnilistele kui äripoole töötajatele.



Joonis 6. Identiteedi- ja juurdepääsuhalduse DevOps teekaart 2022 aastaks

9 akna maatriks (*9 windows matrix*) [Tabel 14] kirjeldab olemasoleva olukorra, magistritöös käsitletava loodava identiteedi- ja juurdepääsuhalduse lahenduse ning tuleviku visiooni süsteemi kolme erineva tasandi (skoobi) abil.

Tabel 14. 9 akna maatriks (*9 windows matrix*) IAM lahenduse ajaline vaade

	Minevik (2020 – 2022)	**Olevik (2022 – 2024)**	**Tulevik (2024 – 2026)**
Peasüsteem (S*upersystem*)	Osaliselt automatiseeritud klientide süsteemide keskkondade lisamise võimekus.	Automatiseeritud klientide süsteemide keskkondade lisamise võimekus.	Automatiseeritud klientide süsteemide keskkondade kustutamise võimekus.
Süsteem (*System*)	Kliendid esitavad kasutajaõiguste haldamiseks tellimusi.	Kliendid on võimelised ise kasutajaõigusi haldama.	Kliendid on võimelised ise kasutajagruppe looma.
Alamsüsteem (*subsystem*)	Kasutajad esitavad identiteedi haldamiseks tellimusi.	Kasutajad on võimelised identiteedi iseteenindust kasutama ja enda seadistusi haldama.	Kasutajad on võimelised ühekordse sisselogimise (SSO) abil autentima erinevatesse rakendustesse.

„Peasüsteem” on kõrgema taseme vaade, mille puhul võib rääkida klientidele eraldatud virtuaaltsoonide kontekstis. „Süsteem” on keskmise taseme vaade, mis kirjeldab selle süsteemi kasutatavust ja peamist funktsionaalsust. „Alamsüsteem” on madalama taseme vaade, mille puhul on mõeldud pisiasju ja konkreetseid funktsionaalsusi, mida klientide kasutajatele pakutakse.

6 Kokkuvõte

Käesoleva magistritöö eesmärk oli käsitleda identiteedi- ja juurdepääsuhalduse äri- ja IT protsesside kitsaskohtade määratlemist ja nende parendamise analüüsi organisatsiooni, meeskondade ja klientide vaatest Tietoevry pilvandmetöötluse äriteenuse suunal. Kirjeldatud on Tietoevry organisatsiooni pilveteenuse pakkumisega seotud projekti äri- ja IT protsesse, mis keskenduvad kasutajaõiguste haldusele ning seda struktureerivale arhitektuurile. Lähtuvalt organisatsiooni ja klientide nõuetest ning eripäradest analüüsiti pilveteenuse juurutamisstrateegiat ning identiteedi- ja juurdepääsuhalduse lahenduse erinevaid tüüpe. Olemasoleva lahenduse puudused on tuvastatud ning nende põhjal kirjeldati probleem ja püstitati ülesanne. Probleemi põhjal on määratud meetrika, mille abil oleks võimalik mõõta lahenduse täiendamise tulemuslikkust. [5]

Autor kirjeldas, modelleeris ja analüüsis probleemi taustsüsteemi, sellega seonduvat meetrikat ja pakkus välja lahenduse, milles uue infosüsteemi analüüsi ja kavandamisega optimeeritakse olemasolevaid ning luuakse uusi protsesse. Lahenduse loomiseks on analüüsitud äri- ja IT protsesse, mille abil oleks võimalik täiendada pilveteenuse olemasolevate ja tulevaste klientide kasutajahalduse tööd. [5] Protsesside parenduste ettepanekud on kirjeldatud ja klientide teenindusvõimekus saaks loodava süsteemiga laiendatud. Olemasolevate klientide ja uute klientide lisandumisel suunatakse teenusepakkuja süsteemihaldurite töökoormus klientidele, millest võidab samuti klient. Lisaks on kirjeldatud aeganõudvate ja veaohtlike haldustööde efektiivsemaks muutmist.

Töö tulemuste hulka kuuluvad kasutajakogemuse täiendamine, haldusõiguste delegeerimisega kaasnevad lisavõimalused ja optimeerimine ning uute klientide pardaletuleku lahenduse kavandamine, mis võimaldab vähendada töömahtu uute süsteemide loomise automatiseerimise juurutamise abil. Samuti hinnatakse loodava tehnilise lahenduse kvaliteedi haldamist. Kavandatava süsteemi saavutatavaid tulemusi on võrreldud probleemi ja nõuete püstitusega ning tehtud tagasivaatavalt lahenduse kavandi suhtes järeldusi.

Magistritöös püstitatud probleem sai lahendatud ja eesmärk täidetud. Planeeritud arendustöödega on reaalselt alustatud ning need jätkuvad. Tulevikus tehtavate arenduste ideed on jõudnud aruteludesse ja nende saavutamise nimel tehakse vajalikke samme.

Kasutatud kirjandus

[1] Tietoevry, Meist, https://www.tietoevry.com/ee/meist/tietoevry-eestis/, 2022.

[2] Tietoevry, Governance, Board of Directors, https://www.tietoevry.com/en/investor-relations/governance/board-of-directors/, 2022.

[3] Tietoevry, Governance, Group management, https://www.tietoevry.com/en/investor-relations/governance/group-management/, 2022.

[4] Tietoevry, Governance, How we are governed, https://www.tietoevry.com/en/investor-relations/governance/how-we-are-governed/, 2022.

[5] M. Sumla, Õppeaine Äriprotsesside haldamine individuaaltöö „Identiteedi- ja juurdepääsuhalduse lahenduse täiustamine jagatud pilveteenuse keskkonna näitel", 2021

[6] Flexera, Cloud Computing Trends: 2021 State of the Cloud Report, https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/#:~:text=The%202021,2020., 2021

[7] NetApp, What is hybrid cloud?, https://www.netapp.com/hybrid-cloud/what-is-hybrid-cloud/#:~:text=The%20primary%20benefit%20of%20a,needs%20for%20a%20competitive%20advantage., 2022.

[8] Tremplin Numérique, Mis on GAIA-X ja miks on kaasatud AWS, Google ja Azure?, https://www.tremplin-numerique.org/et/mis-on-gaia-x-ja-miks-on-seotud-aws-google-ja-azure, 2021

[9] TechTarget, Availability zones, https://searchaws.techtarget.com/definition/availability-zones#:~:text=Availability%20zones%20(AZs)%20are%20isolated,service%20providers'%20data%20centers%20reside.&text=Certain%20cloud%20services%20may%20also%20be%20limited%20to%20particular%20regions%20or%20AZs., 2015.

[10] Riigipilv, Infrastruktuur kui teenus (IaaS), https://riigipilv.ee/teenused/taristu-kui-teenus, 2022.

[11] IBM, SOA Policy, Service Gateway, and SLA Management (First Edition), lk 276, http://www.redbooks.ibm.com/redbooks/pdfs/sg248101.pdf, 2013.

[12] Teenustaseme haldus, SLA sisu, lk 8, Guido Leibur, 2017.

[13] d-Systems, Avatud lähtekoodiga tarkvara, Stabiilsus, turvalisus ja usaldavus, https://www.d-systems.ee/est/OpenSourceSoftware, 2022

[14] LDAP, LDAP Tools, LDAP Browsers and Editors, https://ldap.com/ldap-tools/, 2022.

[15] SWOT & PESTLE, Competitive Analysis of TietoEVRY Oyj, https://www.swotandpestle.com/tietoevry/, 2020.

[16] RSAWEB, Best-effort Internet service and dedicated service, https://www.rsaweb.co.za/best-effort-internet-service-and-dedicated-service/#:~:text=A%20best%2Deffort%20service%20refers,data%20when%20it%20is%20delivered., 2022.

[17] Tietoevry, Our Businesses, Tietoevry Create, https://www.tietoevry.com/en/our-businesses/create/, 2022.

[18] Tietoevry, Investing in Tietoevry, Strategy, https://www.tietoevry.com/en/investor-relations/investing-in-tietoEVRY/strategy/, 2022.

[19] Erik Kralicek, „The Accidental SysAdmin Handbook", lk 235, https://books.google.ee/books?id=VJuFCwAAQBAJ&pg=PA235&lpg=PA235&dq=sysadmin+overhead&source=bl&ots=Gp_dVAud4g&sig=ACfU3U0QZSSrnhDvawTaZXFyumpoucyMWw&hl=en&sa=X&ved=2ahUKEwj4goegnNL2AhXqkosKHfObDNoQ6AF6BAgTEAM#v=onepage&q&f=false, 2016.

[20] James Quick, Toolbox, Identity & Access Management, https://www.toolbox.com/it-security/identity-access-management/guest-article/how-to-measure-the-success-of-iam-deployment/, 2020.

[21] George E. P. Box, „All models are wrong, but some are useful", https://www.lacan.upc.edu/admoreWeb/2018/05/all-models-are-wrong-but-some-are-useful-george-e-p-box/#:~:text=%E2%80%9CAll%20models%20are%20wrong%2C%20but%20some%20are%20useful%E2%80%9D%20is,British%20statistician%20George%20E.%20P.%20Box., 2018.

[22] Elmity, KPI-driven approach to Identity & Access Management, https://www.elimity.com/kpi-driven-approach-to-iam-guide, 2021.

[23] Bob Violino, CSO, 3 IAM deployment models, https://www.csoonline.com/article/3303797/3-iam-deployment-models-which-will-work-for-your-organization.html, 2018.

[24] Paul Fisher, The future of IAM lies in the cloud and as a service, https://ic-consult.com/wp-content/uploads/wp80442_the_future_of_iam_lies_in_the_cloud_and_as_a_service.pdf, 2021.

[25] Tietoevry, Sovereign Cloud, https://www.tietoevry.com/en/services/cloud-and-infrastructure/cloud/sovereign-cloud/, 2022.

[26] Desde Linux, XaaS: Pilvandmetöötlus - kõik teenusena, https://blog.desdelinux.net/et/xaas-pilveteenus-kogu-teenus/, 2022.

[27] Okta, Top 9 Identity & Access Management Challenges with Your Hybrid IT Environment, https://www.okta.com/resources/whitepaper/top-9-iam-challenges-with-your-hybrid-it-environment/, 2022.

[28] Warwick Ashford, ComputerWeekly, How to tackle the IAM challenges of multinational companies, https://www.computerweekly.com/opinion/How-to-tackle-the-IAM-challenges-of-multinational-companies, 2020.

[29] Sagara Gunathunga, WSO2, Here's How IAM Helps With GDPR, https://wso2.com/library/articles/essentials-how-iam-helps-with-gdpr/, 2018.

[30] OpenText, How Identity and Access Management helps meet the data protection requirements of GDPR, https://blogs.opentext.com/how-identity-and-access-management-helps-meet-the-data-protection-requirements-of-gdpr/, 2018.

[31] IT Governance, Data sovereignty and the EU GDPR, https://www.itgovernance.co.uk/data-sovereignty-and-the-cloud, 2022.

[32] Steve Mullan, How to establish your functional requirements for an Identity and Access Management System, Whitehall Media, https://whitehallmedia.co.uk/blog/2016/11/01/establish-functional-requirements-identity-access-management-system/, 2019.

[33] Kristian Roberts, What are IAM Key Processes, https://slideplayer.com/slide/16001214/, 2022.

[34] Michael Brogan, Nathan Dors, University of Washington, RFP Requirements for Identity and Access Management, https://wiki.cac.washington.edu/display/infra/RFP+Requirements+for+Identity+and+Access+Management, 2016.

[35] Gaurav Aggarwal, Multiple cloud perspectives and introduction ot Azure Arc, https://medium.com/gaurav-aggarwal/multiple-cloud-perspectives-and-introduction-to-azure-arc-77fae08f399e, 2021.

[36] Cybernetica, AKIT, Andmekaitse ja infoturbe leksikon, https://akit.cyber.ee/term/513-infoturve, 2022.

[37] Pavel Kodotšigov, „IT teenindussoovide portaali kasutamine IT Service Management rakenduste baasil Tartu Ülikooli Narva Kolledži näitel”, https://digikogu.taltech.ee/et/Download/34fa6402-094b-44da-a349-512847b736cc, 2019.

[38] Bashar Nusebeh, Steve Easterbrook, Requirements Engineering, „Encyclopedia of Physical Science and Technology (Third Edition)”, https://www.sciencedirect.com/referencework/9780122274107/encyclopedia-of-physical-science-and-technology, 2001.

[39] Martin Fowler, BlueGreenDeployment, https://martinfowler.com/bliki/BlueGreenDeployment.html, 2010.

[40] Ucha Vekua, What is Identity Access Management? (IAM), https://www.veriff.com/blog/what-is-identity-access-management, 2021.

[41] ISO/IEC JTC 1/SC 27, ISO/IEC 24760-2:2015, Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements, https://www.iso.org/standard/57915.html, 2015.

[42] ISO/IEC JTC 1/SC 27, ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/standard/54534.html, 2013.

[43] ISO/IEC 27004:2016, Information technology — Security techniques — Information security management Monitoring, measurement, analysis and evaluation, https://www.iso.org/standard/64120.html, 2016.

[44] ISO/IEC JTC 1/SC 27, ISO/IEC 25010:2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, https://www.iso.org/standard/35733.html, 2011.

[45] Joseph Grettenberger, The Fundamentals, Demonstrating a robust ISO 27001 information security management system with identity governance and access management, https://hosteddocs.emediausa.com/demonstrating-a-robust-iso-27001-information-security-management-system-with-identity-governance.pdf, 2017.

[46] Rachel Davies, Non-Functional Requirements: Do User Stories Really Help?, https://www.methodsandtools.com/archive/archive.php?id=113, 2010.

[47] Joost Schalken-Pinkster, Getting non-functional requirements right, https://ictinstitute.nl/getting-non-functional-requirements-right/, 2016.

[48] Jimmy Song, Ignasi Barrera, NGAC Vs RBAC Vs ABAC. https://www.tetrate.io/blog/rbac-vs-abac-vs-ngac/?utm_term=&utm_campaign=Increase+Traffic&utm_source=adwords&utm_medium=ppc&hsa_acc=8582878511&hsa_cam=16384541475&hsa_grp=137482558247&hsa_ad=584073973362&hsa_src=g&hsa_tgt=dsa-1666046905124&hsa_kw=&hsa_mt=, 2021.

[49] Bhavdip Rathod, Best Practices and Benefits of Role Based Access Control, https://www.morganfranklin.com/insights/company-insight/best-practices-and-benefits-of-role-based-permission-control/, 2020.

[50] Guy-Bertrand Kamga, Dealing with Shared Responsibility Model in public Cloud, https://cloudsecurityknowledgesharing.com/dealing-with-shared-responsibility-model-in-public-cloud/, 2018.

[51] The Open Group, 31. Architectural Artifacts, TOGAF Version 9.1, https://pubs.opengroup.org/architecture/togaf9-doc/arch/, 2011.

[52] OCIO, Eight Potential Benefits of Having an IT Architecture, https://ocio.commerce.gov/page/eight-potential-benefits-having-it-architecture#:~:text=An%20architecture%20helps%20an%20organization,reducing%20software%20and%20support%20costs., 20165.

[53] Brian Foote and Joseph Yoder, „If you think good architecture is expensive, try bad architecture.”, Big Ball of Mud, http://www.laputan.org/mud/, 1999.

[54] Stefan Bente, Uwe Bombosch and Shailendra Langade, „Collaborative Enterprise Architecture”, https://www.sciencedirect.com/book/9780124159341/collaborative-enterprise-architecture, 2012.

[55] Cameron, Andrew, and Graham Williamson, „Introduction to IAM Architecture,” IDPro Body of Knowledge, https://bok.idpro.org/article/id/38/, 2020.

[56] Benedict Curtis, How to Build a Minimum Viable Product (MVP): The 2020 Guide, https://dev.to/bencurtis/how-to-build-a-minimum-viable-product-mvp-the-2020-guide-3m4m, 2020.

[57] Visual Paradigm, Effective User Stories - 3C's and INVEST Guide, https://www.visual-paradigm.com/scrum/3c-and-invest-guide/, 2022.

[58] Agile Alliance, Given – When – Then, https://www.agilealliance.org/glossary/gwt/, 2017.

[59] CSS-Tricks, Pidev integreerimine vs pidev kohaletoimetamine vs pidev juurutamine, https://et.csstricks.net/8225202-continuous-integration-vs-continuous-delivery-vs-continuous-deployment, 2022.

[60] Ucha Vekua, What is Identity Access Management? (IAM), https://www.veriff.com/blog/what-is-identity-access-management, 2021.

[61] Palgad, DevOpsi insener, Infotehnoloogia (IT), https://www.palgad.ee/palgainfo/infotehnoloogia-it/devopsi-insener?res_lang=1, 2022.

[62] Palgakalkulaator, Palga ja maksude kalkulaator, https://www.kalkulaator.ee/et/palgakalkulaator, 2022.

[63] Mark Schwartz, The Art of Business Value, 2016.

[64] Archit, Zonka Feedback, https://www.zonkafeedback.com/blog/nps-survey-questions-and-templates, 2019.

[65] Johan Karlsson, Backlog management, Perforce, https://www.perforce.com/blog/hns/4-product-backlog-prioritization-techniques-work, 2018.

[66] Ian Luck, CustomerGauge, https://customergauge.com/blog/how-to-calculate-the-net-promoter-score, 2022.

[67] Jimmy Song, Ignasi Barrera, Why You Should Choose NGAC as Your Access Control Model, https://thenewstack.io/why-you-should-choose-ngac-as-your-access-control-model/, 2021.

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Margus Sumla

1 Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Identiteedi- ja juurdepääsuhalduse lahenduse täiendamine Tietoevry jagatud pilveteenuse keskkonna näitel" mille juhendaja on Nadežda Furs

   1.1 reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

   1.2 üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

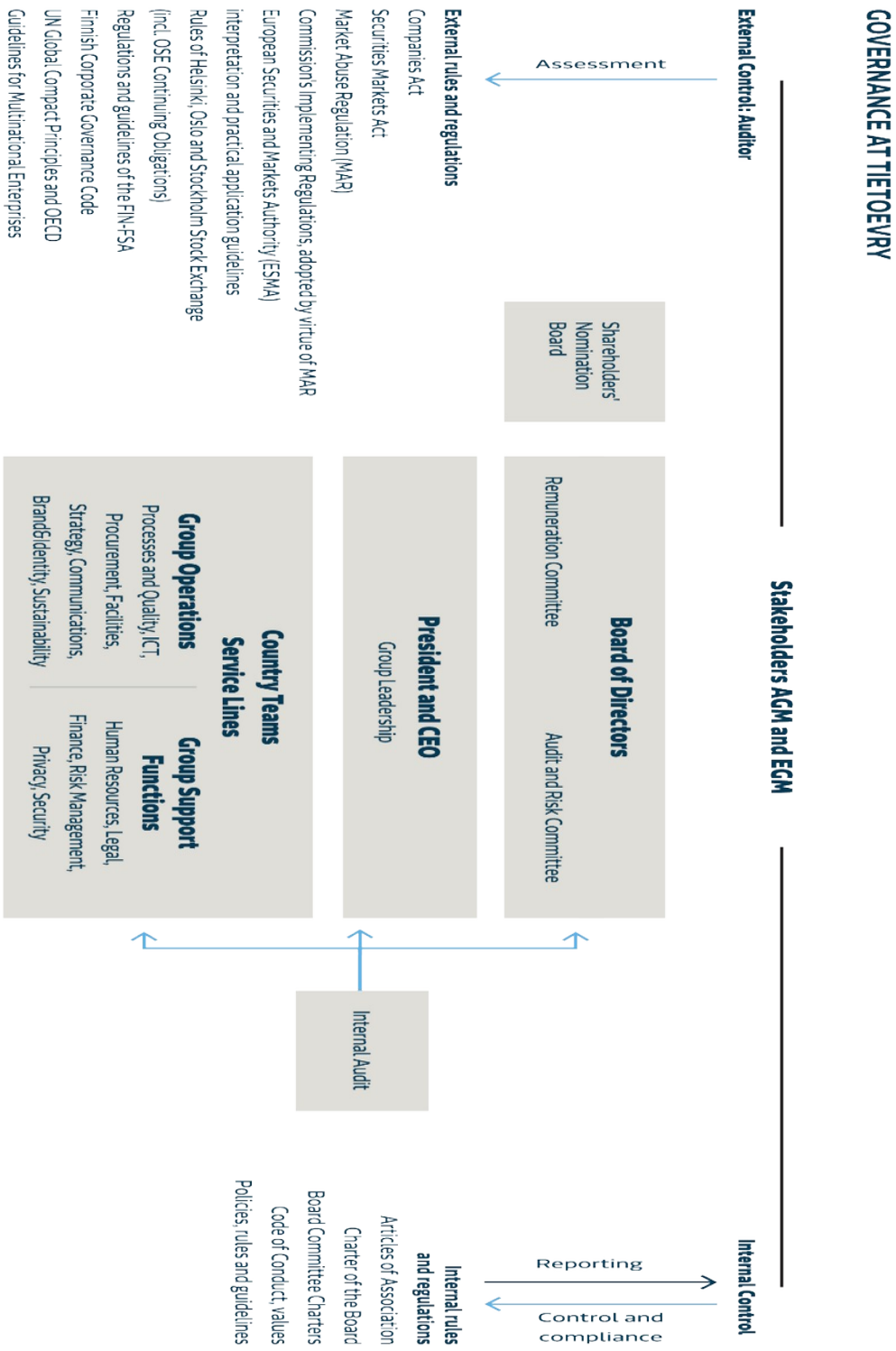
2 Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.

3 Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

19.05.2022

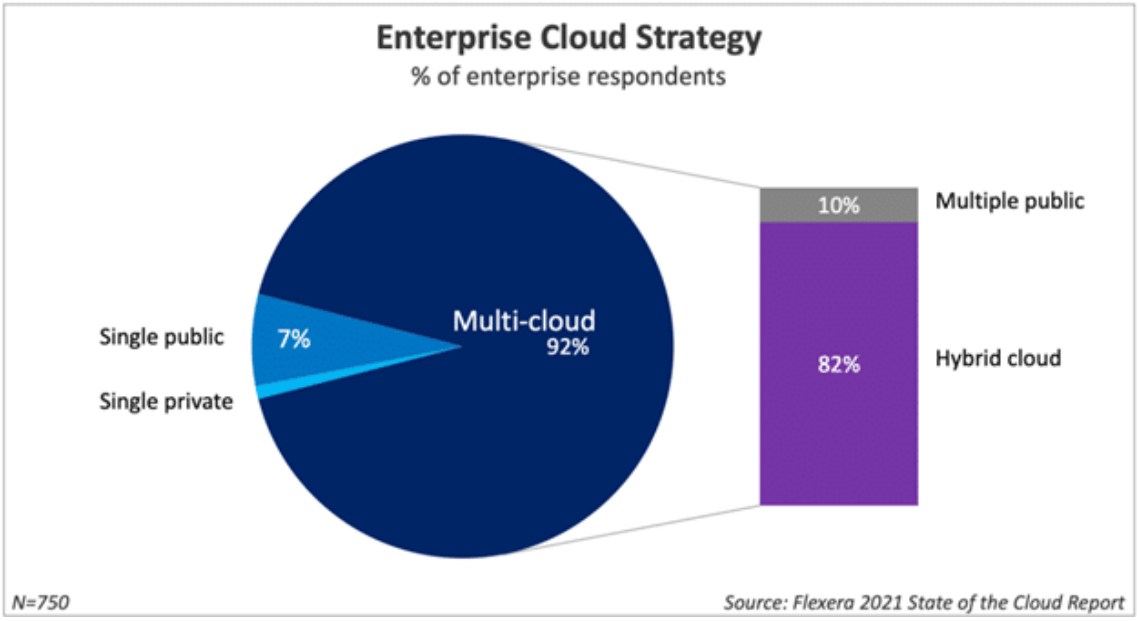
1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2 – Tietoevry valitsemise skeem



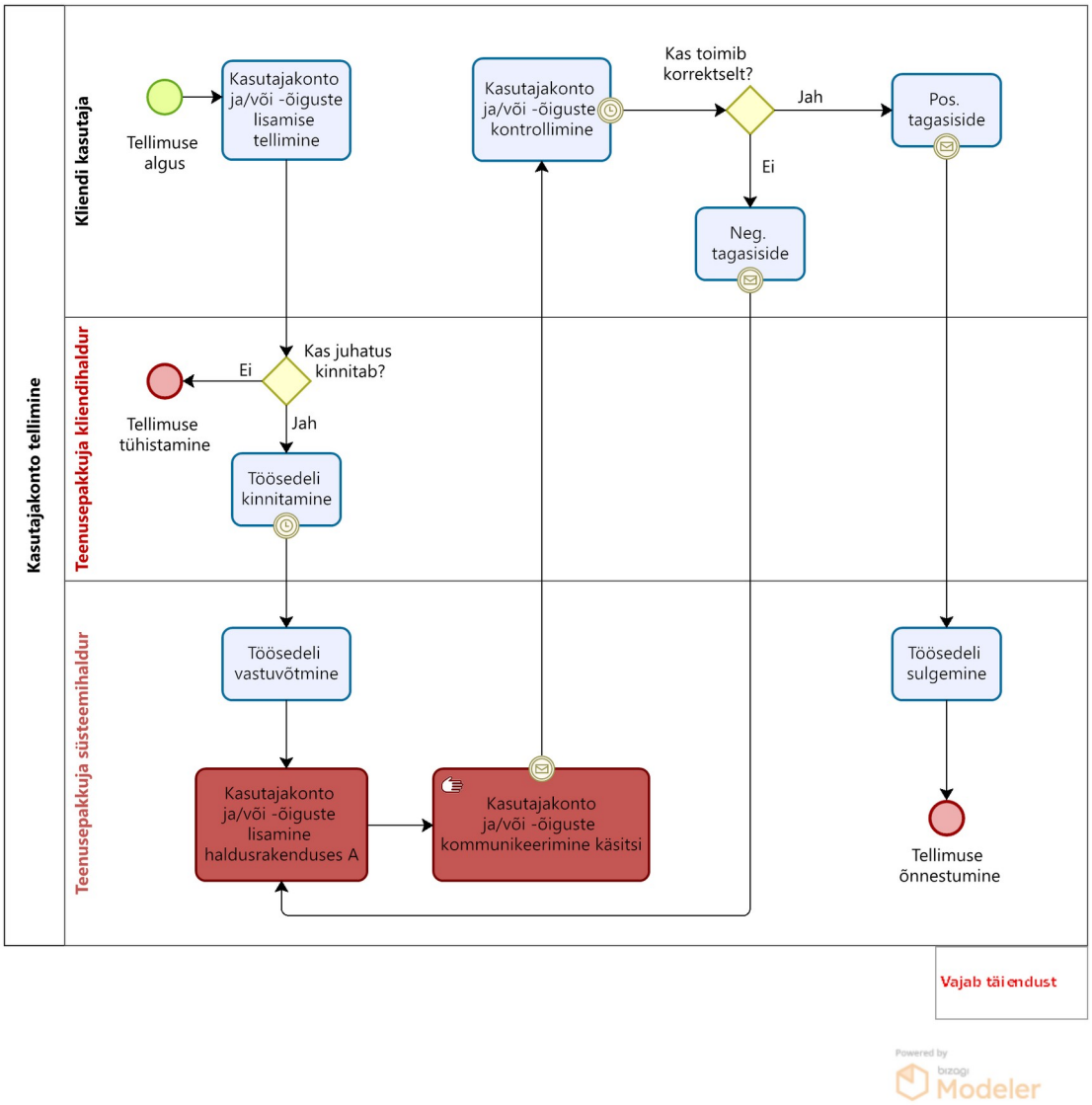
Joonis 7. Tietoevry valitsemise skeem [4]

Lisa 3 – Ettevõtete pilvarvutuse strateegia uuringu ülevaade



Joonis 8. Ettevõtete pilvarvutuse strateegia uuringu ülevaade [6]

Lisa 4 – Identiteedi- ja juurdepääsuhalduse töövoog AS-IS



Joonis 9. Identiteedi- ja juurdepääsuhalduse töövoog AS-IS [5]

Lisa 5 – Identiteedi- ja juurdepääsuhalduse RACI vastutusmaatriks AS-IS

Tabel 15. Identiteedi- ja juurdepääsuhalduse RACI vastutusmaatriks AS-IS [5]

	Kliendi kasutaja	**Teenusepakkuja kliendihaldur**	**Teenusepakkuja süsteemihaldur**
1. Kasutajaõiguste päringu loomine sedelisüsteemi	R, A	C, I	C, I
2. Päringu sedeli kinnitamine	C, I	R, A	C, I
3. Töösedeli vastuvõtmine	C, I	C, I	R, A
4. Kasutajakonto ja/või -õiguste muutmine	I	A, C, I	R, A
5. Sisse logimise info saatmine	I	C	R, A
6. Kasutajaõiguste kontrollimine	R	I	A, C
7. Kasutajaõiguste tagasiside	R, A	I	C, I
8. Töösedeli sulgemine	I	I	R, A
9. Päringu sedeli sulgemine	I	R, A	C, I

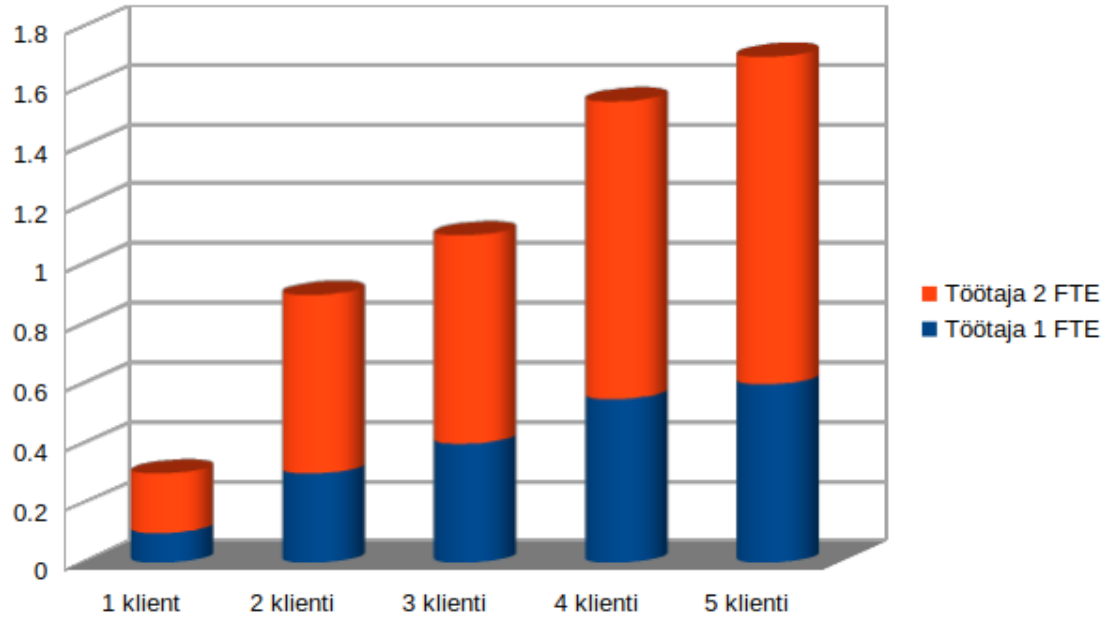
Lisa 6 – Identiteedi- ja juurdepääsuhalduse SIPOC-kaardistus AS-IS

Tabel 16. Identiteedi- ja juurdepääsuhalduse SIPOC-kaardistus AS-IS [5]

Tarnijad (*Suppliers*)	**Sisendid (*Inputs)***	**Protsess (*Process*)**	**Väljundid (*Outputs*)**	**Kliendid (*Customers*)**
Kliendi kasutaja	Tööülesannete tehnilised juhised	1. Kasutajaõiguste päringu loomine sedelisüsteemi	Päringu sedel koos lisainfoga loodud sedelisüsteemi	Teenusepakkuja kliendihaldur
Teenusepakkuja kliendihaldur	Päringu sedel koos lisainfoga loodud sedelisüsteemi	2. Päringu sedeli kinnitamine	Päringu sedel on kinnitatud ja töösedel loodud	Teenusepakkuja haldusmeeskond
Teenusepakkuja haldusmeeskond	Päringu sedel on kinnitatud ja töösedel loodud	3. Töösedeli vastuvõtmine	Töösedel on vastu võetud ja kasutajaõiguste lisamise luba antud	Teenusepakkuja süsteemihaldur
Teenusepakkuja süsteemihaldur	Töösedel on vastu võetud ja kasutajaõiguste lisamise luba antud	4. Kasutajakonto ja/või -õiguste muutmine	Süsteemidele juurdepääs lisatud	Kliendi kasutaja
Teenusepakkuja süsteemihaldur	Süsteemidele juurdepääs lisatud	5. Sisse logimise info saatmine	Sisse logimise info kätte saadud	Kliendi kasutaja
Teenusepakkuja süsteemihaldur	Sisse logimise info kätte saadud	6. Kasutajaõiguste kontrollimine	Kasutajaõigused kontrollitud	Kliendi kasutaja
Kliendi kasutaja	Kasutajaõigused kontrollitud	7. Kasutajaõiguste tagasiside	Kasutajaõiguste kontrollimise tagasiside saadetud	Teenusepakkuja süsteemihaldur
Teenusepakkuja süsteemihaldur	Kasutajaõiguste kontrollimise	8. Töösedeli sulgemine	Töösedel suletud	Teenusepakkuja kliendihaldur

	tagasiside saadetud			

Lisa 7 – Kvalifitseeritud IAM töötajate FTE kumulatsioon klientide vahel AS-IS



Joonis 10. Kvalifitseeritud IAM töötajate FTE kumulatsioon klientide vahel AS-IS

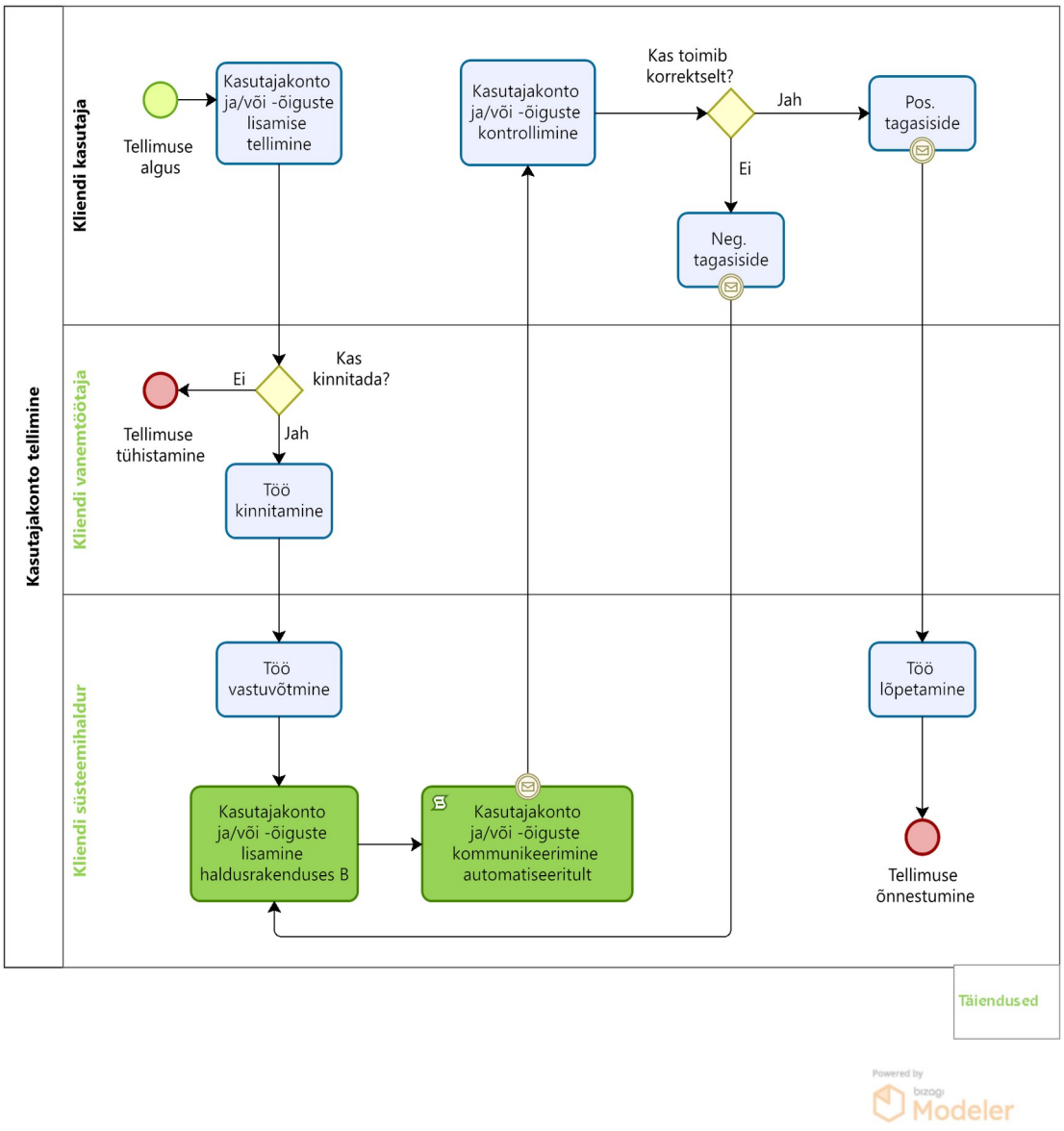
Lisa 8 – Loodava lahenduse funktsionaalsed nõuded

Tabel 17. Loodava lahenduse funktsionaalsed nõuded [5]

Epik	**Kasutaja-lugu**	**Kes?**	**Mida?**	**Miks?**
1	**1**	Mina teenusepakkujana	soovin automatiseeritud identiteedi- ja juurdepääsuhalduse süsteemi juurutamist klientide virtuaaltsoonidesse	selleks, et vähendada probleeme, mis võivad käsitsi serverite konfigureerimisel inimvigate ja -viivituste tõttu tekkida.
1	**2**	Mina teenusepakkujana	soovin automatiseeritud, kiiremat ja optimeeritud kliendi pardaletuleku võimekust	selleks, et oleks võimalik müügitehingute arvu suurendada kiirema väärtuspakkumise loomise abil.
1	**3**	Mina teenusepakkujana	soovin kasutajaõiguste haldamise delegeerida igale kliendile eraldi	selleks, et vähendada süsteemihaldurite töökoormust.
1	**4**	Mina teenusepakkujana	soovin, et iga klient saaks iseenda kasutajate halduse eest vastutada	selleks, et vähendada SLA rikkumisi.
1	**5**	Mina teenusepakkujana	soovin delegeerida kasutajaõiguste päringute kinnitamise või tühistamise kliendi vanemtöötajale	selleks, et kliendi kasutaja saaks kiiremini vajalikud ligipääsuõigused määratud.
2	**6**	Mina kliendi vanemtöötajana	soovin kasutada pilveteenuse juurdepääsu haldusrakenduse iseteenindust delegeeritud administraatori õigustega	selleks, et oleks võimalik säästa kuludelt, mis võivad tekkida ajalisest viitest teenusepakkuja ja kliendi vahelise informatsiooni käsitsi vahetamisel.
2	**7**	Mina kliendi vanemtöötajana	soovin vastutada pilveteenuse juurdepääsu päringute kinnitamise või	selleks, et oleks võimalik kiiremalt ostetud teenust kasutama hakata.

			tühistamise eest	
3	8	Mina kliendi kasutajana	soovin kasutada pilveteenuse juurdepääsu haldusrakenduse iseteenindust	selleks, et säästa aega parooli taastamisega iseseisvalt.
3	9	Mina kliendi kasutajana	soovin kasutajaliideses vajalikke lahtreid	selleks, et redigeerida enda isiklikke andmeid ja seadistust.

Lisa 9 – Identiteedi- ja juurdepääsuhalduse töövoog TO-BE



Joonis 11. Identiteedi- ja juurdepääsuhalduse töövoog TO-BE [5]

Lisa 10 – Identiteedi- ja juurdepääsuhalduse RACI vastutusmaatriks TO-BE

Tabel 18. Identiteedi- ja juurdepääsuhalduse RACI vastutusmaatriks TO-BE [5]

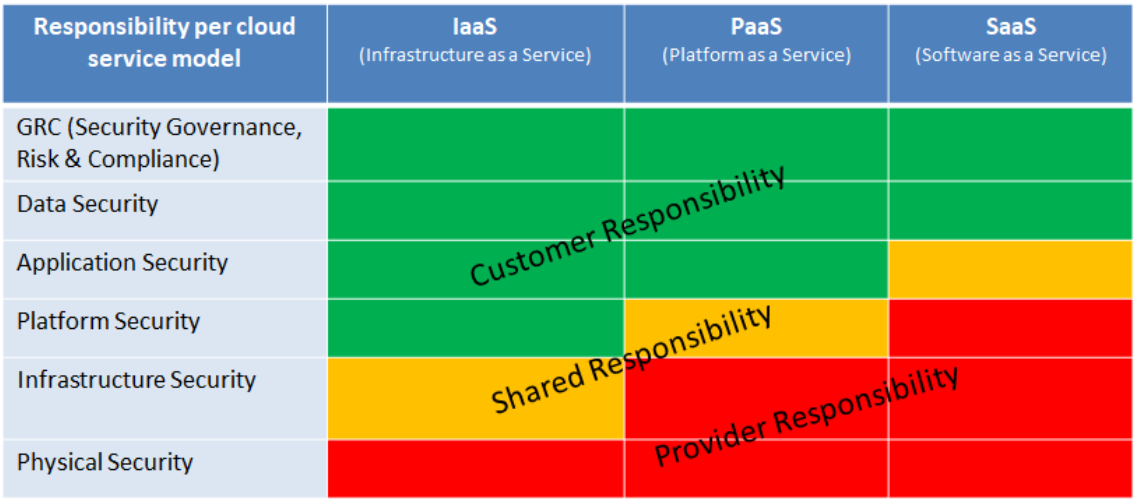
	Kliendi kasutaja	**Kliendi vanemtöötaja**	**Kliendi süsteemihaldur**
1. Kasutajaõiguste päringu loomine sedelisüsteemi	R, A	C, I	C, I
2. Päringu sedeli kinnitamine	C, I	R, A	C, I
3. Töösedeli vastuvõtmine	C, I	C, I	R, A
4. Kasutajakonto ja/või -õiguste muutmine	I	A, C, I	R, A
5. Sisse logimise info saatmine	I	C	R, A
6. Kasutajaõiguste kontrollimine	R	I	A, C
7. Kasutajaõiguste tagasiside	R, A	I	C, I
8. Töösedeli sulgemine	I	I	R, A
9. Päringu sedeli sulgemine	I	R, A	C, I

Lisa 11 – Identiteedi- ja juurdepääsuhalduse SIPOC-kaardistus TO-BE

Tabel 19. Identiteedi- ja juurdepääsuhalduse SIPOC-kaardistus TO-BE [5]

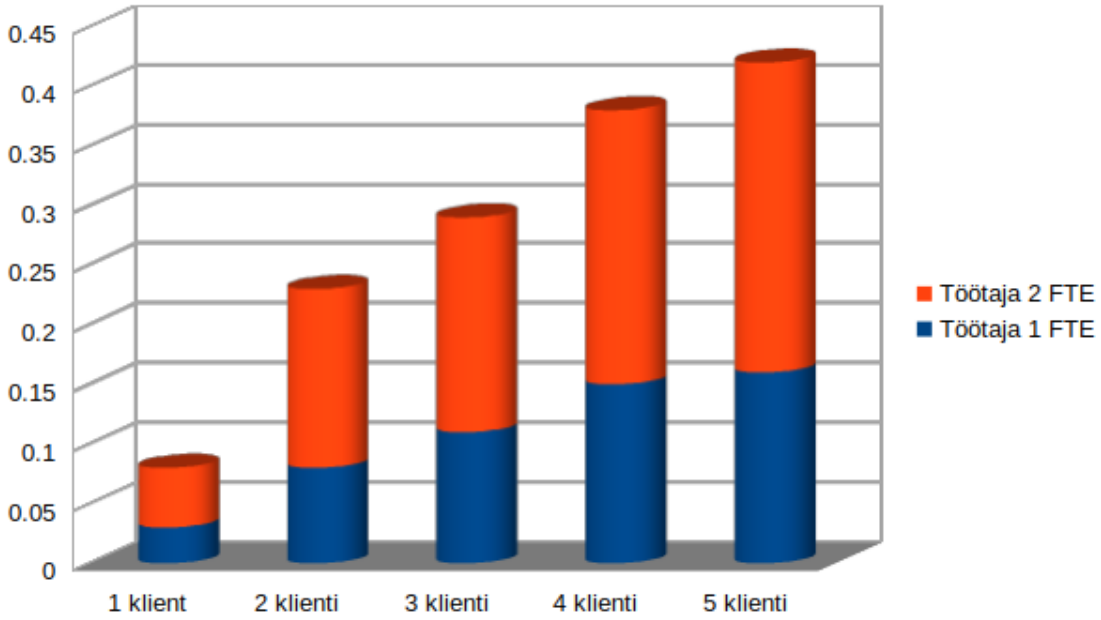
Tarnijad (*Suppliers*)	**Sisendid (*Inputs)***	**Protsess (*Process*)**	**Väljundid (*Outputs*)**	**Kliendid (*Customers*)**
Kliendi kasutaja	Tööülesannete tehnilised juhised	1. Kasutajaõiguste päringu loomine sedelisüsteemi	Päring koos lisainfoga edastatud	Kliendi vanemtöötaja
Kliendi vanemtöötaja	Päring koos lisainfoga edastatud	2. Päringu kinnitamine	Päring on kinnitatud	Kliendi süsteemihaldur
Kliendi süsteemihaldur	Päring on kinnitatud	3. Töö vastuvõtmine	Töö on vastu võetud ja kasutajaõiguste lisamise luba antud	Kliendi süsteemihaldur
Kliendi süsteemihaldur	Töö on vastu võetud ja kasutajaõiguste lisamise luba antud	4. Kasutajakonto ja/või -õiguste muutmine	Süsteemidele juurdepääs lisatud	Kliendi kasutaja
Haldusrakendus B	Süsteemidele juurdepääs lisatud	5. Sisse logimise info saatmine	Sisse logimise info kätte saadud	Kliendi kasutaja
Kliendi süsteemihaldur	Sisse logimise info kätte saadud	6. Kasutajaõiguste kontrollimine	Kasutajaõigused kontrollitud	Kliendi kasutaja
Kliendi kasutaja	Kasutajaõigused kontrollitud	7. Kasutajaõiguste tagasiside	Kasutajaõiguste kontrollimise tagasiside saadetud	Kliendi süsteemihaldur
Kliendi süsteemihaldur	Kasutajaõiguste kontrollimise tagasiside saadetud	8. Töö lõpetamine	Töö lõpetatud	Kliendi vanemtöötaja

Lisa 12 – Pilveteenuse pakkuja ja kliendi jagatud turbe vastutus



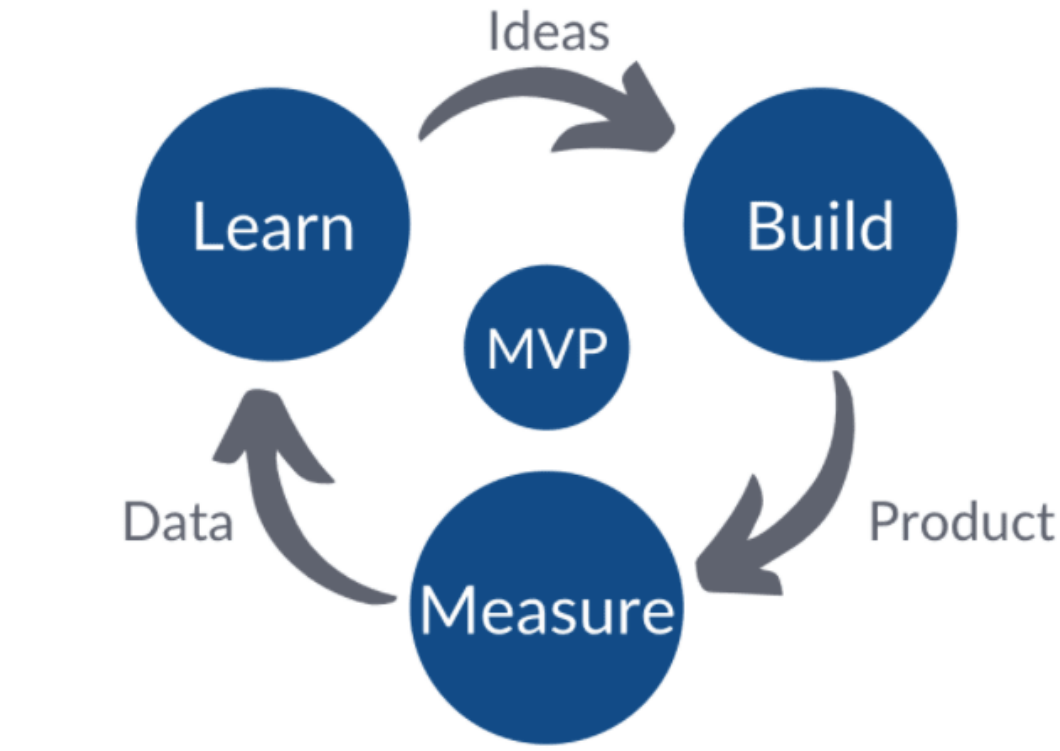
Joonis 12. Pilveteenuse pakkuja ja kliendi jagatud turbe vastutus [50]

Lisa 13 – Kvalifitseeritud IAM töötajate FTE kumulatsioon klientide vahel TO-BE



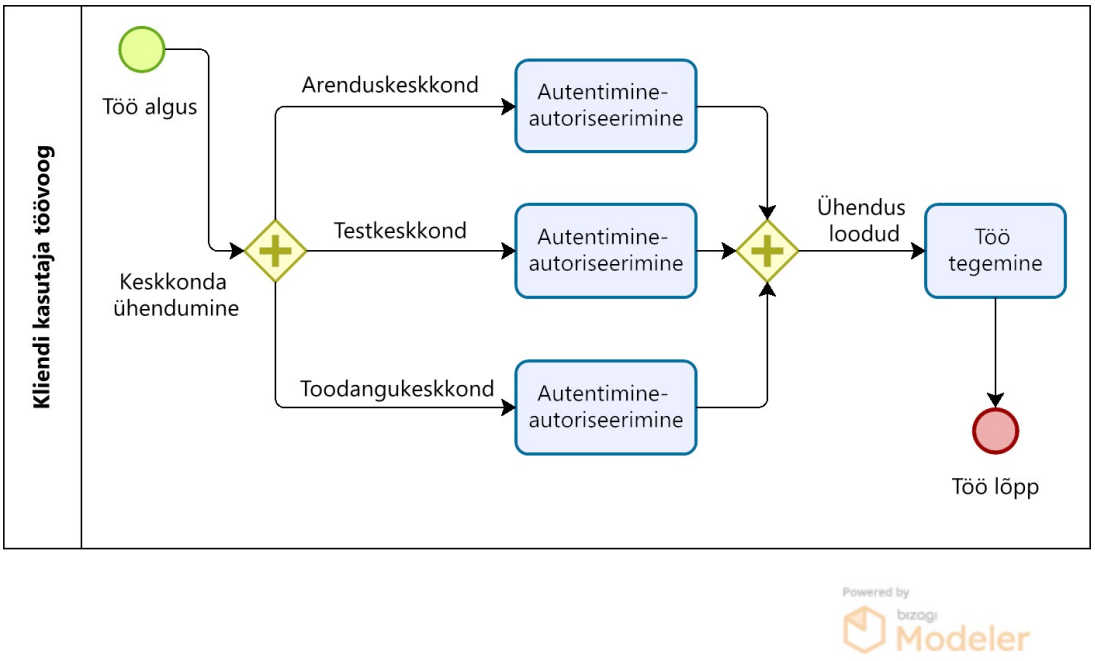
Joonis 13. Kvalifitseeritud IAM töötajate FTE kumulatsioon klientide vahel TO-BE

Lisa 14 – MVP meetodi skeem



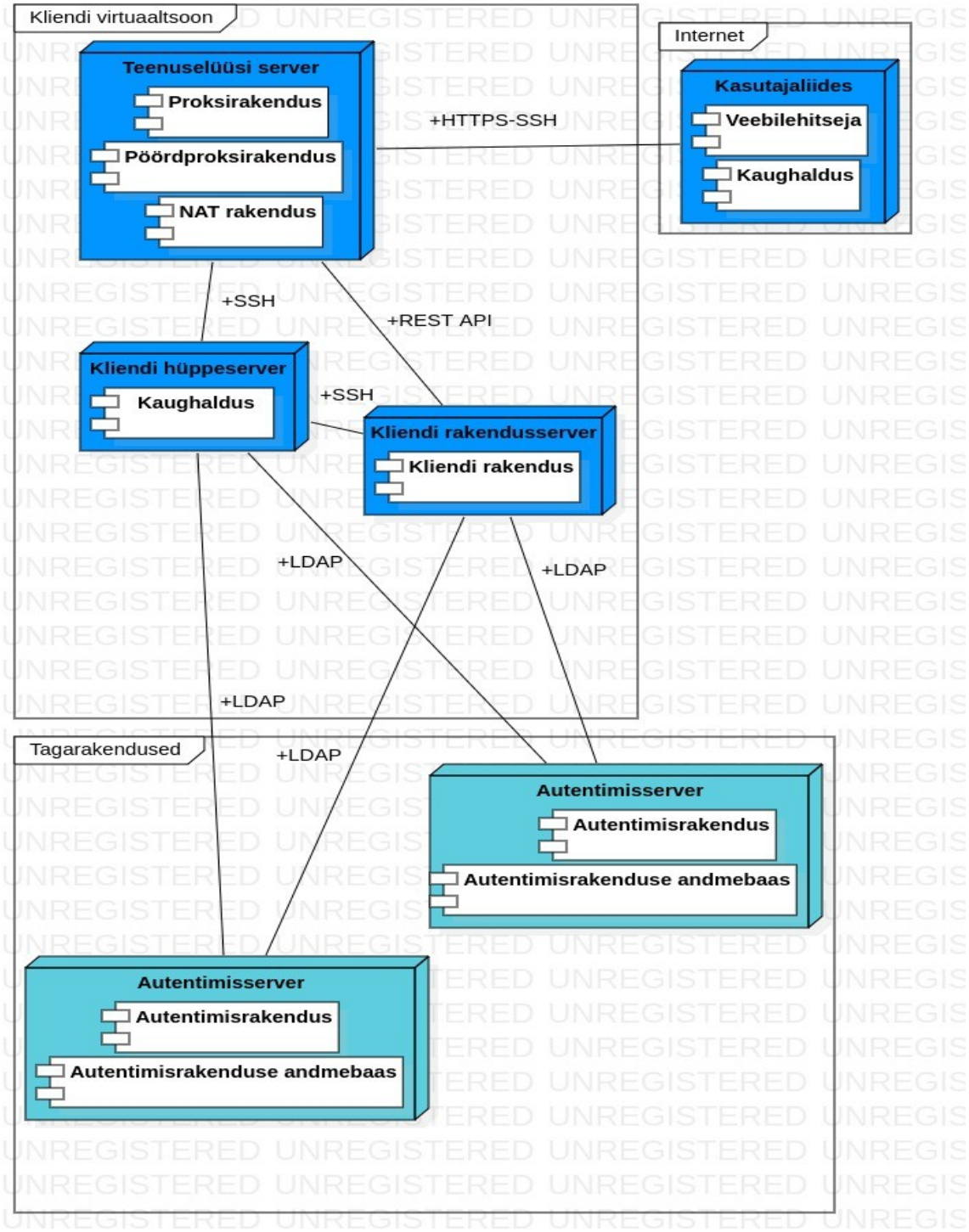
Joonis 14. MVP meetodi skeem [56]

Lisa 15 – Kliendi kasutaja töövoog pilveplatvormi virtuaaltsooni keskkonnas



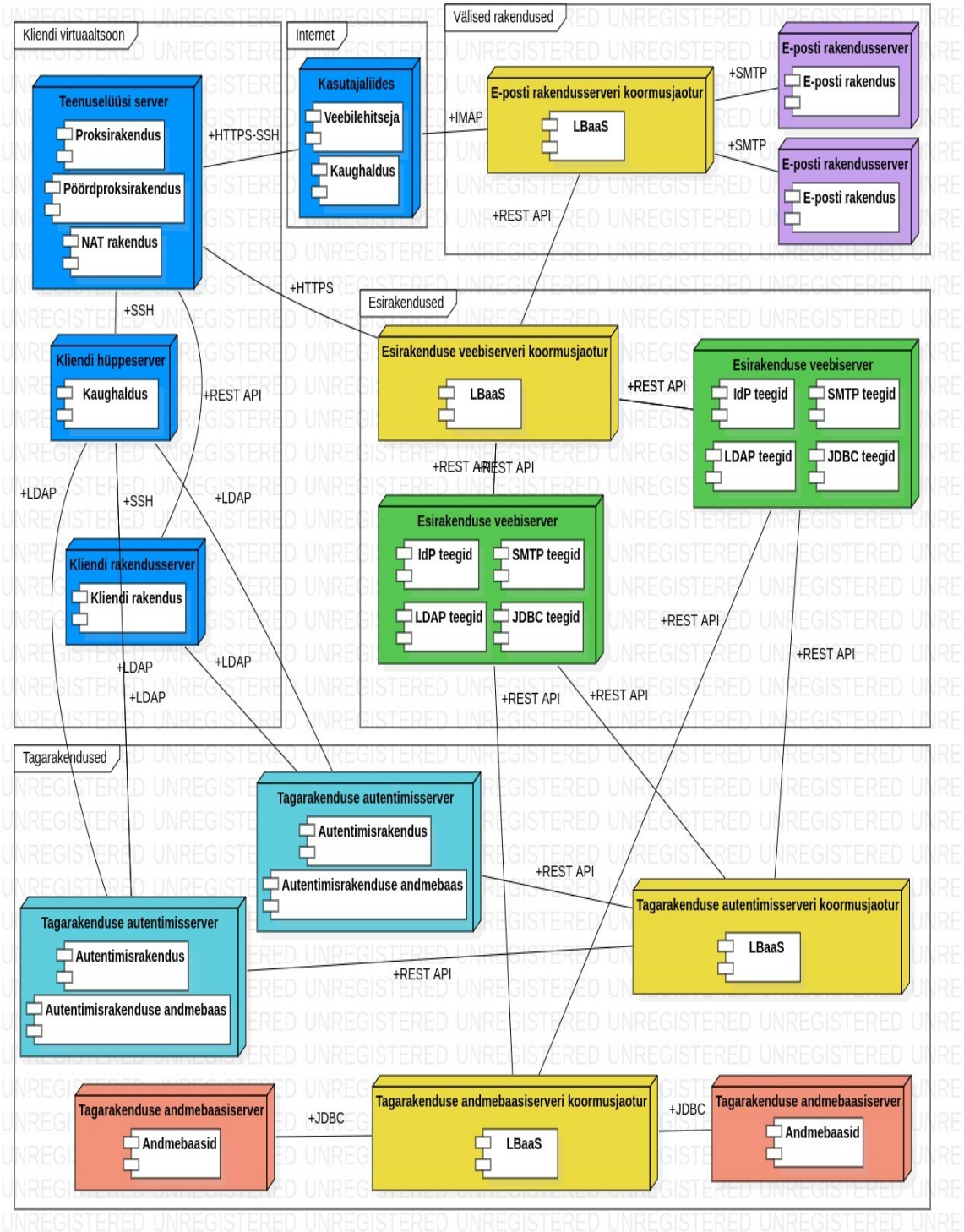
Joonis 15. Kliendi kasutaja töövoog pilveplatvormi virtuaaltsooni keskkonnas

Lisa 16 – IAM süsteemi evitusdiagramm AS-IS



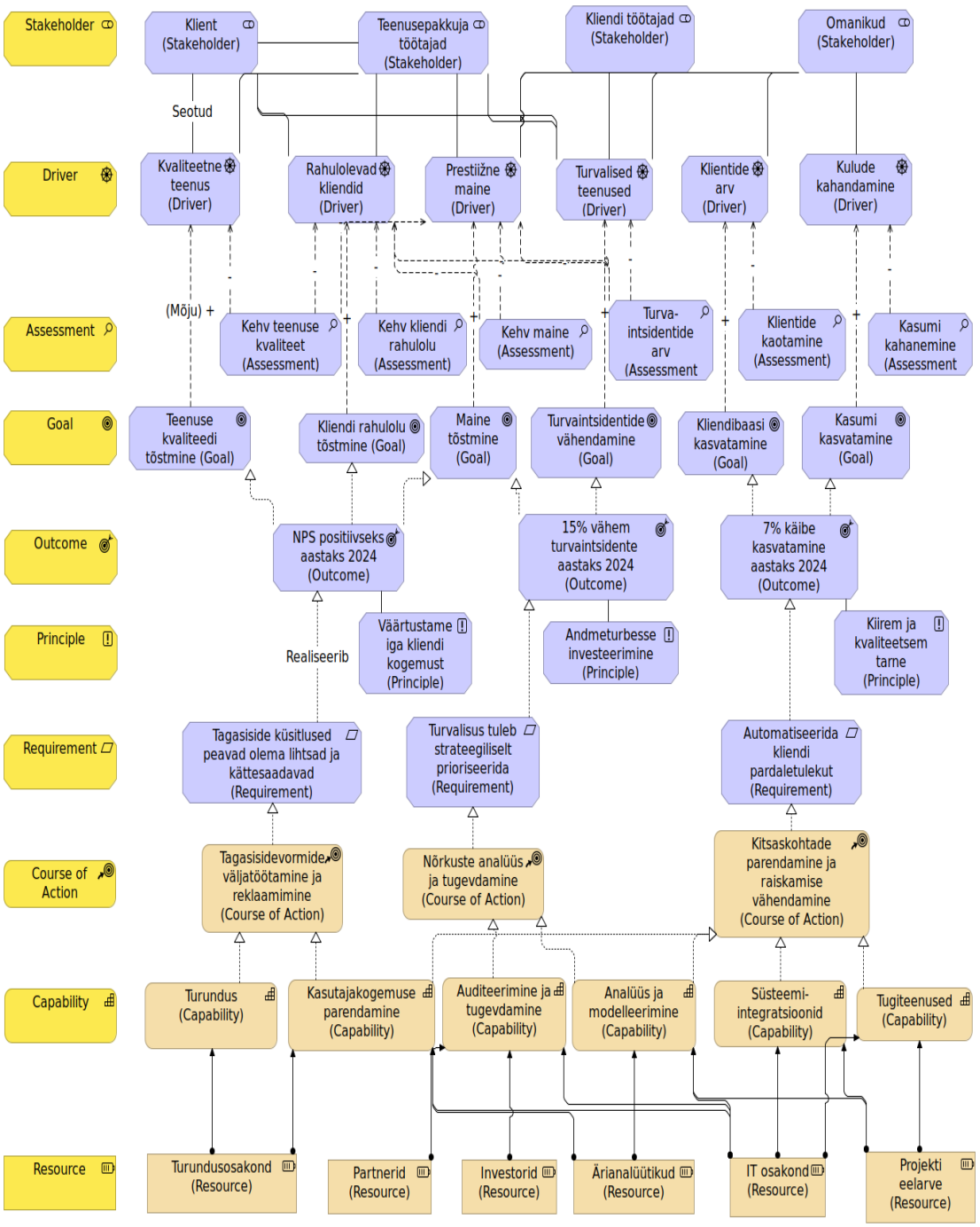
Joonis 16. Identiteedi- ja juurdepääsuhalduse süsteemi evitusdiagramm AS-IS

Lisa 17 – IAM süsteemi evitusdiagramm TO-BE



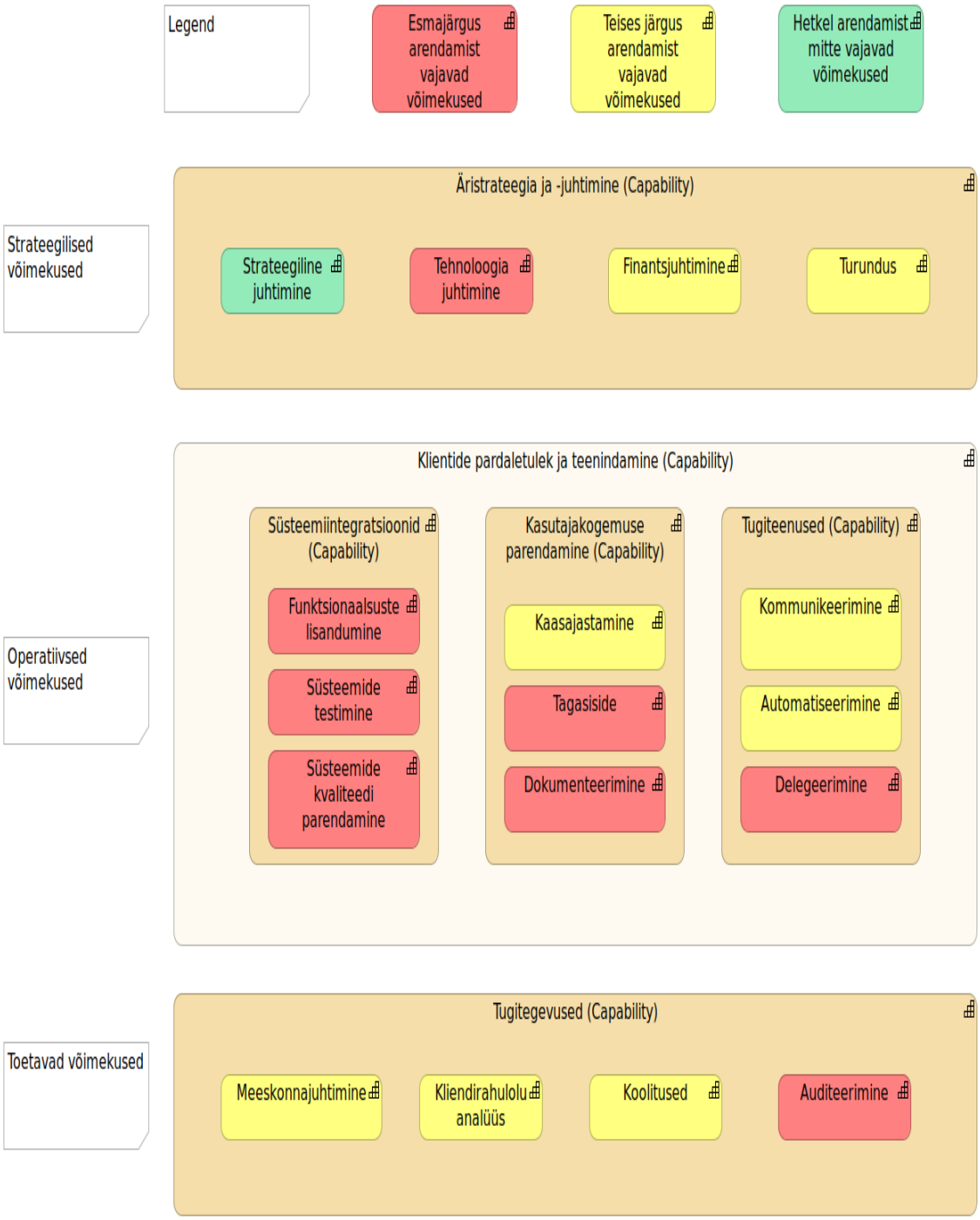
Joonis 17. Identiteedi- ja juurdepääsuhalduse süsteemi evitusdiagramm TO-BE

Lisa 18 – IAM äriteenuse motivatsiooni- ja strateegiamudel



Joonis 18. IAM äriteenuse motivatsiooni- ja strateegiamudel

Lisa 19 – IAM ärivõimekuste ülevaate kaart



Joonis 19. IAM ärivõimekuste ülevaate kaart

Lisa 20 – IAM äriteenuse tagasiside küsitluse tulemused

Tabel 20. IAM äriteenuse tagasiside küsitluse tulemused [64]

	Tenant 1 and tenant 2 (average values and highlights)
1. On the scale of 1 to 10, how would you rate your experience using our managed infrastructure (IaaS) cloud services?	▪ 9 (25%), 8 (25%), 7 (25%), 5 (25%) ▪ Average: 7.25 ▪ NPS: 0
2. On the scale of 1 to 10, how would you rate your experience accessing our cloud service resources?	▪ 9 (25%), 8 (25%), 6 (25%), 5 (25%) ▪ Average: 7 ▪ NPS: -25
3. On the scale of 1 to 10, how satisfied are you with our support services?	▪ 9 (25%), 8 (25%), 7 (25%), 5 (25%) ▪ Average: 8 ▪ NPS: 0
4. On the scale of 1 to 10, how satisfied are you with our cloud's operational documentation?	▪ 9 (50%), 5 (50%) ▪ Average: 7 ▪ NPS: 0
5. On the scale of 1 to 10, how satisfied are you with the onboarding process of a new infosystem environment using our cloud services?	▪ 9 (50%), 7 (25%), 4 (25%) ▪ Average: 6.25 ▪ NPS: 25
6. Based on your recent experience please rate how long it took you to gain user	▪ A few days (50%)

permissions to a specific environment or application?	▪ Less than a day (25%) ▪ More than a week (25%).
7. Would you find it beneficial to order and handle access management within your organisation instead at the service provider's when accessing our cloud services?	▪ I find it beneficial to order my account and access permissions directly from my manager (25%) ▪ I find it beneficial to order my account and access permissions directly from my team lead/senior engineer (50%) ▪ I find it beneficial to order my account and access permissions from the service provider (25%)
8. What do you like least about the services we provide?	▪ Speed (20%) ▪ User experience (40%) ▪ Support services (20%) ▪ Information and documentation (20%)
9. What do you like most about the services we provide?	▪ Quality (10%) ▪ Speed (10%) ▪ Technologies used (20%) ▪ Attitude (10%) ▪ Staff (30%) ▪ Security (10%) ▪ Support services (10%)
10. How could we improve your experience?	▪ Generally I'm satisfied.

	▪ More self service tools or visibility to the environment. ▪ Bigger team.

Lisa 21 – Kasutajaõiguste ja -rollide reguleerimise mudelite võrdlus

	Pros	Cons
ABAC	+ Flexibility	x Performance and auditability can be problematic
RBAC	+ Simplicity	x Role explosion x Fixed access rights x Challenges meeting regulatory requirements
NGAC	+ High level of granularity + Auditability + Flexibility + Combined access policies	x Complexity

Joonis 20. Kasutajaõiguste ja -rollide reguleerimise mudelite võrdlus [67]