Karina Tumanova

APPLE TÖÖJAAMADE HALDUS MITME DOMEENIVÕRGUGA SUURETTEVÕTTES

LÕPUTÖÖ

Teenusmajanduse instituut
Teabehalduse ja infosüsteemide korraldamise õppekava
Juhendajad: Meelis Rebane, MA
Edward Salmus, BA
Mart Reinla

Mõdriku 2023

SISUKORD

AUTORI DEKLARATSIOON JA LIHTLITSENTS

Mina, **Karina Tumanova**, tõendan, et lõputöö on minu kirjutatud. Töö koostamisel kasutatud teiste autorite, sh juhendaja teostele on viidatud õiguspäraselt.

Kõik isiklikud ja varalised autoriõigused käesoleva lõputöö osas kuuluvad autori/te/le ainuisikuliselt ning need on kaitstud autoriõiguse seadusega.

Juhendaja **Meelis Rebane** */allkirjastatud digitaalselt/*

Juhendaja **Edward Salmus** */allkirjastatud digitaalselt/*

Juhendaja **Mart Reinla** */allkirjastatud digitaalselt/*

Lõputöö on kaitsmisele lubatud teenusmajanduse instituudi direktori korraldusega nr 1-14/53 kuupäev 03.05.2023.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, **Karina Tumanova** sünnikuupäev: **06.12.2001** annan Tallinna Tehnikakõrgkoolile (edaspidi kõrgkool) tasuta loa (lihtlitsentsi) enda loodud teose **Apple tööjaamade haldus mitme domeenivõrguga suurettevõttes.**

1. reprodutseerimiseks paberkandjal kõrgkooli raamatukogus avaldamise ja säilitamise eesmärgil;
2. elektroonseks avaldamiseks kõrgkooli repositooriumi kaudu;
3. kui lõputöö avaldamisele on instituudi direktori korraldusega kehtestatud tähtajaline piirang, lõputöö avaldada pärast piirangu lõppemist.

Olen teadlik, et nimetatud õigused jäävad alles ka autorile ja kinnitan, et:

1. lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid ega muid õigusi;
2. PDF-failina esitatud töö vastab täielikult kirjalikult esitatud tööle.

Mõdrikul, 03.05.2023 */allkirjastatud digitaalselt/*

LÜHENDID

ABM *(Apple Business Manager)* – Apple'i seadmete haldamiseks loodud teenus (Valge Klaar, 2018)

MDM *(Mobile Device Management* – mobiilseadmete haldus, olemuselt tarkvara andmete ja konfiguratsioonide haldamise korraldamiseks (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

VPP (*Volume Purchase Program*) – rakenduste ning raamatute litsentside hulgi ostmiseks loodud programm (Apple Inc., 2017)

E-ITS – Eesti infoturbestandard, mis on eestikeelne ja Eesti õigusruumile vastav infoturbe käsitlemise alus (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

macOS *(Macintosh operating system)* – 2001. aastal loodud operatsioonisüsteem firmalt Apple Inc, mis põhineb graafilisel kasutajaliidesel (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

FURPS – *(Functionality, Usability, Reliability, Performance, Supportability)* metoodika tarkvaraarenduse nõuete klassifitseerimiseks (Jamwal, 2010)

CERT-EE – infoturbeintsidentide käsitlemise osakond (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

CIS Level 2 – *(Center for Internet Security, Level 2),* prioritiseeritud kogum tegevusi, mis üheskoos moodustavad parimate tavade kogumi eesmärgiga leevendada kõige levinumaid rünnakuid IT-süsteemide ja võrkude vastu (*Center fot Internet Security, Inc,* 2019)

PoLP *(Principle of least privilege)* – minimaalõiguste printsiip, mille põhimõtteks on anda kasutajakontodele ainult need õigused, mida nad vajavad oma töö edukaks tegemiseks. (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

XML *(Extensible Markup Language)* – laiendatav märgistuskeel (AKIT - *Andmekaitse ja infoturbe leksikon*, 2022)

BYOD *(Bring Your Own Device)* – poliitika, mis lubab ettevõttes kasutada tööseadmena töötaja isiklikke seadmeid (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

iOS – Apple'i loodud nutitelefonides kasutatav mobiil-operatsioonisüsteem (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

tvOS – Apple TV's kasutatav operatsioonisüsteem

SSO *(Single Sign-On)* – *f*unktsioon, mis võimaldab kasutajal ühe sisselogimisega pääseda ligi mitmetele ressurssidele (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

agiilne arendus – tarkvaraarenduse metoodika, välearendus (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

inkrement – lõpetatud tööd, mis lisatakse eelnevatele inkrementidele, moodustades seeläbi tervikliku ja kasutatava toote

OS X – operatsioonisüsteemi macOS versioon 10 (2012) (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

Deploy – protseduur toote kasutuselevõtuks organisatsioonis (*AKIT - Andmekaitse ja infoturbe leksikon*, 2022)

PAM (*Privileged Access Management*) – identiteediturbelahendus ehk eriõigustega kontode haldamine (*What Is Privileged Access Management (PAM) | Microsoft Security*, s.a.)

SISSEJUHATUS

2021. aasta nimetati Riigi Infosüsteemi Ameti poolt Eestis turvanõrkuste aastaks, kus võidujooksus aja ja kurjategijatega tuli võtta vastu valusaid õppetunde (*Küberturvalisuse aastaraamat 2022*, 2022). Järgmisel aastal ei läinud olukord paremaks ning värskelt ilmunud RIA aastaraamatus (*Küberturvalisuse aastaraamat 2023*, 2023) nimetati 2022. aasta ummistusrünnete aastaks, ründajate sihtmärkideks olid ka Eesti meediaettevõtted. 2022. aastal registreeris CERT-EE 2627 mõjuga intsidenti, 2021. aastal registreeris CERT-EE kokku 390 intsidenti vähem ehk 2237 mõjuga intsidenti, nimetatud aasta aprillis teavitati ka suuremast juhtumist, kus sihiti IT-teenust pakkuvat ettevõtet ning selle kaudu sai lunavaraga pihta veel neli ettevõtet. Kokkuvõtvalt näitavad toimunud intsidendid, et turvanõrkused, konfiguratsioonivead ning vananenud tarkvara võimaldavad küberrünnakuid, millel on mõju meie igapäevaelule ning tööle.

Tõsiseks probleemiks organisatsioonides on taakvara ehk *legacy* hoidmine, tegu on süsteemidega, mis töötavad, kuid on oma aja ära elanud ning on kergesti rünnatavad (*Küberturvalisuse aastaraamat 2022*, 2022). Sarnaselt taakvarale võivad ka ajale jalgu jäänud tööprotsessid kujutada endast ohtu organisatsiooni seadmete turvalisusele – üheks selliseks ohuks võib pidada ühtse seadmete keskhaldussüsteemi puudumist. Olukord, kus kasutajate seadmeid tuleb käsitsi seadistada, puudub ülevaade ettevõtte varadest ning seire seadmete olukorra üle, tarkvara uuendamine on tülikas ning tihtilugu jäetud tahaplaanile ja seetõttu kasutatakse seadmetes tihti vananenud või turvanõrkustega tarkvara.

Ettevõtetes on seadmete turvalise haldamise üheks parimaks praktikaks mobiilseadmete halduse kasutamine (ingl *mobile device management*, MDM), tänu millele on võimalik erinevaid konfiguratsiooniprofiile kasutades oluliselt maandada turvalisuse riske ning parandada ka seadmete kasutusmugavust ettevõtte töötaja silmis (Trudel, 2016).

MDM tarkvara kasutamine võimaldab seadmeid keskselt konfigureerida ja hallata vastavalt etteantud nõuetele. Haldustarkvara kasutamise eeliseks on võimekus rakendada tööjaamadele ühtseid turvapoliitikaid, kontrollida seadmete olekut, keelata kindlaid funktsioone ning ka kasutajate küsimuste ja murede lahendamine on tunduvalt mugavam, paljusid probleeme saab ennetada juba seadmete monitooringu käigus (seadme oleku seire) – näiteks on vananenud tarkvaraga tööjaamad märgistatud ja neile on võimalik kohe tähelepanu pöörata. Pahavararünnaku korral on samuti keskhaldussüsteemist tulev kasu väga suur – kui pahavara leitakse ühes tööjaamas, on võimalik

vastumeetmeid käivitada korraga kõikides teistes seadmetes (Veldre, 2016). Niisamuti toetavad osad keskhaldusteenused kasutajate turvalist autentimist klientarvutites.

Lõputöö on loodud Ekspress Grupi Apple seadmete keskhaldusesse juurutamise projekti käigus. 2020. aastal juurutati meediakontsernis Apple tööjaamade keskhaldustarkvara Mosyle Business, kuhu on järk-järgult seadmeid ka lisatud. Kontsernil on aga mitu tütarettevõtet, kus on kasutusel erinevad Windows domeenid, kuid võimekus lisada Apple seadmeid keskhaldusesse on seni vaid kindlal tütarettevõttel – Delfi Meedial. Tööjaamade keskhaldussüsteemi lisamisel puudub hetkel võimalus valida mitme Windows domeeni vahel, mis takistab ülejäänud tütarettevõtetes seadmete keskhalduse juurutamist.

Lõputöö eesmärk on luua kontsernis kasutusel olevasse keskhaldussüsteemi uus funktsionaalsus, tänu millele on kasutajatel võimalik ennast macOS seadmetes erinevatest domeenidest autentida, et tekiks võimalus macOS keskhalduse juurutamiseks ka teistes kontserni tütarettevõtetes, tõhustades seeläbi küberturvalisust ning kasutusmugavust.

Lõputöö eesmärgi saavutamiseks püstitas töö autor järgmised ülesanded:

- kirjeldada olemasolev süsteem *(as-is)*;
- analüüsida tütarettevõtetes kasutatava tööprotsessi vastavust E-ITS infoturbestandardile ning määrata projekti ajakava;
- kaardistada lisatava funktsionaalsuse nõuded;
- prioritiseerida kaardistatud nõuded;
- valida sobiv arendusmetoodika;
- luua ja juurutada funktsionaalsus mitmest domeenist autentimiseks;
- teha ettepanekuid keskhaldustarkvara edasiseks parendamiseks.

Lõputöö käigus peetakse mitmeid koosolekuid ning arutelusid IT-toe töötajatega – nii kaardistatakse lisatava funktsionaalsuse nõuded ja hetkel olemasoleva protsessi kitsaskohad. Saadud sisendite ajendil valiti sobiv arendusmetoodika.

Lisatava funktsionaalsuse nõuete kirjeldamiseks kasutab töö autor FURPS metoodikat ning prioritiseerimiseks MoSCoW meetodit. Kontserni tütarettevõtetes kasutusel olevat Apple tööjaamade haldust analüüsitakse kasutades E-ITS infoturbestandardit.

Lõputöö esimeses peatükis kirjeldatakse lõputöö metoodikat, teises peatükis antakse ülevaade meediakontsernist Ekspress Grupp ning kirjeldatakse Apple tööjaamade käsitsi seadistamise tööprotsessi ja keskhaldussüsteemi lisamise protsessi. Kolmandas peatükis kirjeldatakse Apple tööjaamade keskhalduse teoreetilised lähtekohad ning kontsernis kasutatavat haldustarkvara. Neljandas peatükis loetletakse lisatava funktsionaalsuse nõuded ning prioritiseeritakse need. Viiendas peatükis kirjeldatakse projekti loomiste, testimise ja juurutamise teoreetilisi ning metoodilisi lähtekohti. Kuuendas peatükis kirjeldab töö autor uue funktsionaalsuse loomist ja juurutamist ning viimases peatükis teeb ettepanekud keskhaldussüsteemi edasiseks parendamiseks.

1 LÕPUTÖÖ METOODIKA

Lõputöö põhiosa on struktureeritud vastavalt teemade loogilisele järjestusele, kõik peatükid on eelnevate peatükkidega seotud. Esimestes peatükkides on kirjeldatud teoreetilised ja metoodilised lähtekohad. Seejärel on antud ülevaade lisatava funktsionaalsuse loomisest, testimisest ja implementeerimisest ning viimases peatükis on toodud välja autoripoolsed ettepanekud keskhalduse edasiseks arendamiseks.

Kontsernis arvuti käsitsi seadistamise (*as-is*) ning keskhaldusesse lisamise (*to-be*) tööprotsesside loomiseks kasutatakse lõputöös BPMN (*Business Process Modelling Notation*) modelleerimismeetodit – protsessijoonised on loodud kasutades Camunda modelleerimise platvormi. BPMN valiti seetõttu, et selle abil on lihtne selgelt ja visuaalselt kujutada ettevõttes toimivaid tööprotsesse.

Lõputöös kujutatud joonised on loodud kasutades Figma ning MindNode disainitööriistu. Figma on pilvepõhine rakendus, tänu millele on jooniseid võimalik jooksvalt muuta ning nendele alati ligi pääseda. MindNode on mugav rakendus mõttekaartide (*mind map*) ning ajurünnakute (*brainstorming*) läbiviimiseks – kasutades MindNode rakendust kirjeldati lisatava funktsionaalsuse nõuded. Kõik joonised ja tabelid, millel puudub viide on lõputöö autori koostatud.

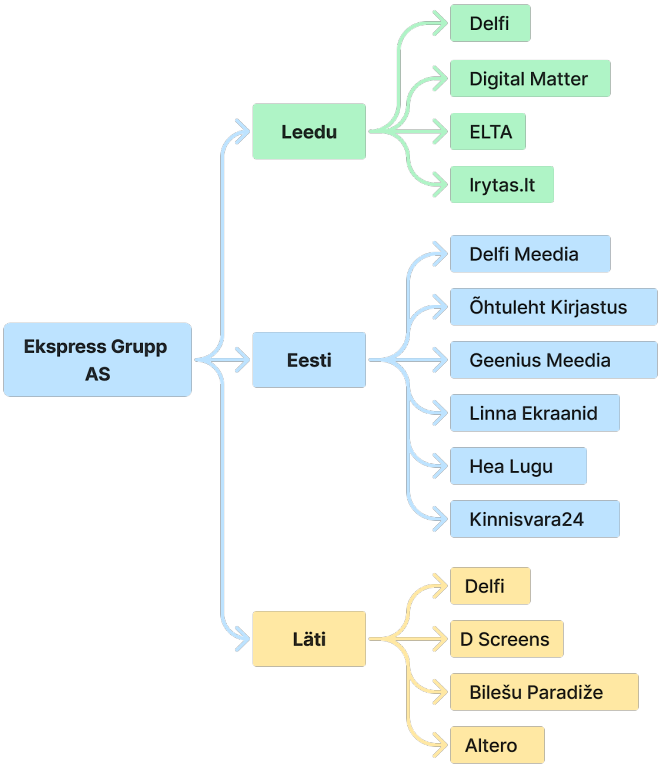
Kontserni tütarettevõtetes arvutite käsitsi seadistamise tööprotsessi (*as-is*) ja arvuti edasist kasutust analüüsis autor lähtudes E-ITS infoturbestandardile. E-ITS osutus valituks, kuna standard on eestikeelne ning kooskõlas ISO/IEC 27001 standardiga.

Lisatava funktsionaalsuse nõuete kaardistamiseks ning klassifitseerimiseks kasutati laialtlevinud FURPS metoodikat, sest see võimaldab struktureeritult kirjeldada erinevaid tarkvaranõudeid, tagades seeläbi nii funktsionaalsuse kvaliteet kui ka kasutajakogemus. Eelnevalt kaardistatud nõuete prioritiseerimiseks kasutati lõputöös MoSCoW meetodit, sest nii on võimalik selgelt välja tuua nõuded, mida on kindlasti vajalik täita ning kirjeldada ka vähemolulised nõuded, mille täitmine ei ole antud ajahetkel kohustuslik.

Lõputöö käigus kasutati lisatava funktsionaalsuse loomiseks agiilset lähenemisviisi, sobilikuks valiti Scrum raamistik, kuna see keskendub eelkõige meeskonnatööle ning paindlikkusele ja võimaldab erinevates töö etappides vajadusel sisse viia muudatusi. Funktsionaalsuse testimiseks kasutati sprintide käigus musta kasti testimist (*black box testing*), mis võimaldas testida funktsionaalsust kasutades kasutajaliidest.

2 MEEDIAKONTSERNI EKSPRESS GRUPP TUTVUSTUS JA APPLE TÖÖJAAMADE HALDUSE ANALÜÜS TÜTARETTEVÕTETES (*AS-IS*)

AS Ekspress Grupp on Eestis 1989. aastal loodud kontsern, kuhu tänaseks kuulub mitmeid meediaettevõtteid Eestis, Lätis ja Leedus, lisaks ka erinevad veebiportaalid ning digimeedialahendusi pakkuvad ettevõtted. Joonisel 1 on välja toodud Ekspress Grupile kuuluvad ettevõtted. Kontserni põhitegevuseks on ajakirjandusliku sisu tootmine, reklaami müük digitaalsetele platvormidele, piletimüügikohtade ja piletimüügi ning ajalehtede, raamatute ja ajakirjade kirjastamine. Kontserni peamisteks fookusteks on kujunenud digitaalsete lahenduste ja teenuste arendamine. „Grupi ettevõtted haldavad pea terviklikku meediasisu ahelat alates sisuloomest kuni trüki, kojukande ja klienditeeninduseni välja. Meie põhitegevusi toetavad grupisiseselt juhitav infotehnoloogia arendus, audiovisuaalse produktsiooni lahendused, reklaamipindade müük väliekraanidel“ (Ekspress Grupp AS, 2022). Ekspress Grupi peamisteks klientideks on meediasisu tarbijad, reklaamiostjad ning ettevõtete teenuseid ostvad kliendid (AS Ekspress Grupp, 2022). Tänaseks pakub kontsern Baltimaades tööd ligikaudu üle 1600 inimesele.



Joonis 1. Ekspress Grupp ning selle tütarettevõtted Leedus, Eestis ja Lätis

Ekspress Grupi eesmärkideks on (Ekspress Grupp AS, 2022):

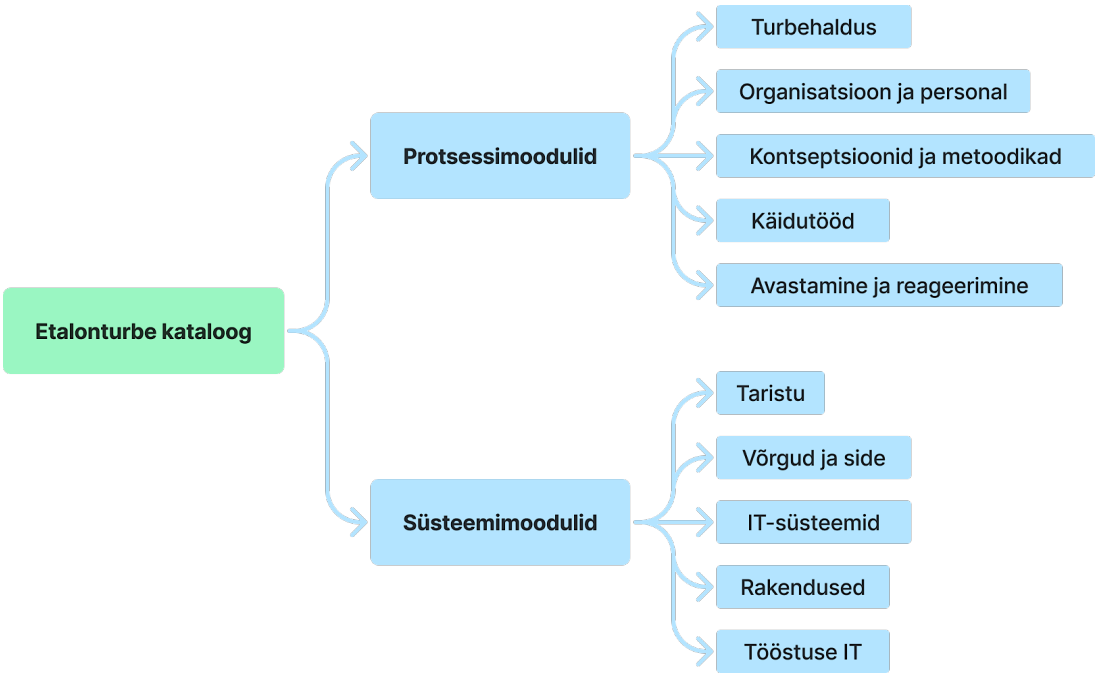
- olla Baltimaade juhtiv digikirjastaja;
- luua auhinnatud sisu;
- pakkuda paberkandjal kvaliteetseid meediaväljaandeid;
- tegutseda sotsiaalset vastutust silmas pidades ning luua tugevaid ja usaldusväärseid brände.

Meediakontsernis hallatava arvutipargi suuruseks on Eestis ligikaudu 500 tööjaama, millest 300 arvutit on Windows operatsioonisüsteemiga ning 200 arvutit macOS operatsioonisüsteemiga. Selleks, et oleks võimalik kontsernis hoida ühtset tööjaamade haldamise põhimõtet, kasutatakse arvutite süsteemseks haldamiseks keskhaldustarkvarasid – Microsoft Endpoint Configuration Manager (Windows seadmete jaoks) ning Mosyle Business (Delfi Meedia Apple seadmete jaoks).

2.1 Apple tööjaamade haldus kontserni tütarettevõtetes

Apple tööjaamade haldamiseks on keskhaldustarkvara kasutusel vaid ühel tütarettevõttel – Delfi Meedial, teistes tütarettevõtetes ei ole Apple seadmed keskselt hallatud. Apple tööjaamade käsitsi seadistamise protsessi ning edasise kasutuse analüüsimisel kasutas autor E-ITSi etalonturbe kataloogi. E-ITS (senine infoturbesüsteem ISKE) on 2022. aastal jõustunud uus Eesti infoturbestandard, mis põhineb Saksa etalonturbe süsteemil BSI IT-Grundschutz (BSIG) ja on kooskõlas rahvusvahelise infoturbehalduse standardiga ISO/IEC 27001. E-ITS on eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks, mille eesmärgiks on korraldada ja tagada avalike ülesannete täitmiseks vajalike infosüsteemide ja ka äriprotsesside kaitse. E-ITSi missiooniks on ka arendada ja edendada Eestis tegutsevate erafirmade infoturbe taset. Eesti infoturbestandardit haldab Riigi Infosüsteemi Amet, see on tasuta kättesaadav ning selle sisu uuendatakse iga-aastaselt (*E-ITS Tutvustus*, s.a.). Majandus- ja kommunikatsiooniministeeriumi 2022. aasta lõpus avaldatud pressiteates väitis RIA peadirektori asetäitja Gert Auväärt, et uus standard on kasulik ning vajalik abivahend turvariskide kaardistamiseks ja küberturvalisuse taseme tõstmiseks (Pihlak, 2022).

Etalonturbe kataloogis on jaotatud ohtude tõrjeks kasutatavad meetmed mooduliteks. Moodulid jagunevad kaheks: süsteemimoodulid ning protsessimoodulid (*Eesti Infoturbestandard*, s.a.). Moodulite sisu on kirjeldatud joonisel 2 (lk 13).



Joonis 2. Etalonturbe kataloogi jaotus moodulitena (*E-ITS Tutvustus*, s.a.)

Protsessimoodulite põhiteemadeks on: turbehaldus, organisatsioon ja personal, kontseptsioonid ja metoodikad, käidutööd ning avastamine ja reageerimine. Süsteemimoodulite põhiteemadeks on: taristu, võrgud ja side, IT-süsteemid, rakendused ja tööstuse IT. Keskne sülearvutite haldus ehk MDM on defineeritud Eesti infoturbestandardis (E-ITS) mobiilseadmete halduse põhimõttena (süsteemimoodulid, IT-süsteemide peatükis) ning on määratud kõrgeimaks meetmeks sülearvutite turvalisuse tagamisel (*SYS.3.2.2: Mobiilseadmete haldus (MDM)*, s.a.). Kontserni tütarettevõtete seadmeid, mida hetkel ei ole võimalik liidestada keskhaldussüsteemiga valmistatakse kasutajatele üleandmiseks ette käsitsi. Uue töötaja tööle asumisest antakse IT-osakonnale teada ligikaudu paar nädalat ette, seejärel veendutakse, kas uuele töötajale on sobilikud seadmed olemas ja nende puudumisel tehakse uus tellimus. Peale seadmete saabumist algab arvuti seadistamise protsess mida viib läbi IT-tehnik, *as-is* tööprotsessiga on võimalik detailsemalt tutvuda Lisas 1 (lk 52).

Lähtuvalt E-ITS etalonturbe kataloogile analüüsis autor Apple arvutite käsitsi seadistamise tööprotsessi (*as-is*) ja arvuti edasist kasutust. Töövoo kitsaskohad, nende lahendus kasutades MDM tarkvara ning viide E-ITS kataloogile on kirjeldatud joonisel 3 (lk 14).

Nr	Kitsaskoha kirjeldus	Võimalike riskide selgitus	Lahendus kasutades MDM teenust	Viide E-ITSis
1	Käsitsi seadistatud tööjaamu ei uuendata korrapäraselt (rakendused ning operatsioonisüsteem).	Uuendamata rakendused ja operatsioonisüsteem on väga ohtlikud - klientarvuti on haavatav kahjurvara suhtes.	Läbi MDM süsteemi toimub pidev macOS-i ja rakenduste uuendamine.	**SYS.2.4.M1** macOS-i turvalise rakendamise kava
2	Administreerivate õigustega tavakasutaja konto ei ole macOS seadmetes hallatud	Konfigureerimise käigus tavakasutajale loodud administreerivate õigustega konto jääb tema kasutusse - nii saab kasutaja seadmesse alla laadida kõike, mida soovib, ka pahavara.	Kasutades MDM süsteemi puuduvad kõikidel kasutajatel administreerivad õigused	**SYS.2.4.M3** Kasutajakontode haldus [kasutaja]
3	Puudub tööjaamade aktiivne seire.	Puudub teadmine seadme töövõimest ning probleemidest	MDM süsteemis aktiivselt seiratakse tööjaamu ning teavitatakse probleemide korral.	**SYS.2.1.M29** Klientarvutite seire
4	Puudub turvaseadete haldus.	Turvaseadeid ei ole keskselt kirjeldatud, puudub turvalisus.	MDM süsteemis toimib keskne turvaseadete haldus.	**SYS.2.1.M44** Keskne klientarvutite turvaseadete haldus
5	Seadmed ei ole keskselt hallatud.	Puudub ülevaade seadmetest, nende kasutajatest ning olukorrast.	MDM tarkvara võimaldab saada seadmetest ja nende olukorrast ning kasutajatest ülevaadet	**SYS.3.1.M16** Keskne sülearvutite haldus (C-I)
6	Seadme varguse/kadumise korral ei ole võimalik kaugelt seadet kustutada.	Kasutajanime ja parooli teades on võimalik andmetele ligipääseda.	MDM süsteemis on võimalik arvuti kaugelt minuti jooksul lukustada ja kustutada.	**SYS.2.4.M11** Seadme turvaline kõrvaldamine
7	Allalaaditud rakendusi kasutatakse suuremate õigustega, kui tarvis.	Suureneb rakenduse vastu suunatud ründe tõenäosus ning õnnestumine.	Seadmete ettevalmistamiseks ja rakenduste installimiseks kasutatakse Apple Business Manageri.	**SYS.3.2.3.M12** Apple ID anonüümimine
8	Administreerivate õigustega kasutajakontod saavad installeerida erinevat tarkvara.	Tavakasutajad ei oska ette näha riske internetist tarkvara allalaadimisel ning on suur oht pahavaraga nakatumiseks.	MDM süsteemis saab tavakasutaja installeerida rakendusi kasutades Self-Service rakendust, vaikimisi on internetist rakenduste allalaadimine keelatud.	**SYS.2.1.M33** Rakenduste käitamise tõkestamine (C-I)
9	Puudub keskne ülevaade ettevõtte Apple seadmetest.	Ettevõttes puudub ülevaade kõigist seadmetest.	MDM süsteem tagab ülevaate kõigist kasutusel olevatest seadmetest.	**OPS.1.1.2.M20** Seadmete korrakohane kasutuselevõtt
10	Lokaalsetel kasutajakontodel puuduvad kindlad paroolinõuded.	Lihtsate paroolidega kontosid on kergem kaaperdada.	Läbi MDM süsteemi on kirjeldatud kindlad paroolinõuded.	**OPS.1.2.4.M2** Kaugtööarvuti turve

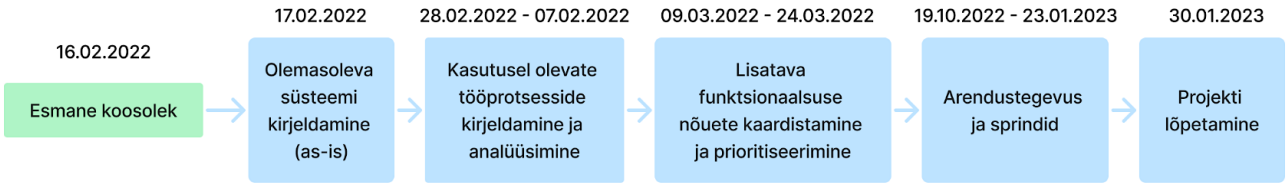
Joonis 3. Apple tööjaamade iseseisva haldamise kitsaskohad ning nende lahendused

Autor analüüsis kokku 10 erinevat kitsaskohta, põhjendas võimalikke riske ning pakkus välja lahenduse kasutades MDM tarkvara – lähtuvalt joonisel 3 väljatoodust on kõik kirjeldatud kitsaskohad võimalik lahendada kasutades MDM tarkvara. Peale analüüsi koostas autor arvuti keskhaldusesse lisamise tööprotsessi (*to-be*) joonise (Lisa 2, lk 53).

2.2 Juurutusprojekti ajakava

Juurutusprojekt sai alguse 2022. aasta veebruaris. 16. veebruaril arutasid autor ning IT-süsteemide administraator koosolekul probleeme olemasolevas süsteemis ning tõdesid, et on vaja luua uus funktsionaalsus, mis võimaldaks erinevatest domeenidest kasutajatel ennast macOS seadmetes autentida. 09. märtsil 2022 toimus teine koosolek, kus arutati lisatava funktsionaalsuse nõudeid ning seal osales lisaks autorile ja IT-süsteemide administraatorile ka IT-kasutajatoe juht. Nädal aega hiljem 23. märtsil prioritiseeriti koosolekul eelnevalt kirja pandud nõuded ja autor lõi ka nõuete prioritiseerimise tabeli.

Projekti arendus toimus kokku kolmes kahenädalases sprindis, testimist teostati iga sprindi jooksul. Projekt lõpeb 2023. aasta jaanuaris funktsionaalsuse kasutusele võtmisega. Joonisel 4 on välja toodud projekti üldine ajakava.



Joonis 4. Projekti üldine ajakava

Lisas 3 (lk 54) on võimalik tutvuda projekti ajakavaga detailsemalt.

3 APPLE TÖÖJAAMADE KESKHALDUSE TEOREETILISED LÄHTEKOHAD (*AS-IS*)

IT-turbe üheks aspektiks on andmete ligipääsu piiramine vajaliku miinimumini, mis kujutab endast rakendusprogrammide ning süsteemihalduse programmide kasutamise võimaldamist vaid nendele töötajatele, kes neid ligipääse tõepoolest vajavad. Antud põhimõtte kohaselt tuleks vajalikud volitused koguda kokku volituste profiilidesse ning neile toetudes luua kasutajagrupid (*Infoturbe soovituste juhend*, 2009). Andmekaitse ja infoturbe leksikoni järgi nimetatakse sellist pääsupoliitika põhimõtet PoLP printsiibiks, mille kohaselt saav isik mingite objektide kasutamiseks minimaalsed õigused, mida ta vajab. Keskhalduse *(Mobile Device Management, MDM)* kasutamine annab ettevõttele suurepärase võimaluse rakendada seadmetes turvapoliitikaid ning juurutada ja kasutada grupipõhist ligipääsupoliitikat erinevatele masinapõhistele ressurssidele. Andmetele ligipääsemise ohu korral on võimalik seade tühjendada äriandmetest ilma, et oleks vaja füüsiliselt arvutit puutuda (näiteks kui seade kaob või seade varastatakse) (Oixio AS, 2021). Mobiilseadmete keskhaldus on justkui katustermin kõikidele loodud teenustele ning tehnoloogiatele, mis võimaldavad mis tahes seadmeid keskselt ning eemalt hallata (Dreyer & Karneboge, 2016). „Mobiilseadmete keskhaldus annab ettevõttele kontrolli seadme üle.“ (Oixio AS, 2021)

Turu-uuringute ettevõte MarketsandMarkets 2022. aastal koostatud uuringu „Mobile Device Management Market by Component (Solutions (Device management, Application Management, Security management) and Services), Deployment Mode, Organization Size, Operating system Vertical and Region - Global Forecast to 2026“ kohaselt on lähiaastatel oodata ettevõtetes keskhaldustarkvarade laialdasemat kasutuselevõttu, mis sai alguse Covid-19 pandeemia puhangust. Üle maailma pidid ettevõtete töötajad jääma järsku kodukontoritesse ning sellega avastasid palju IT-töötajad, kui keeruline on ilma keskhalduseta sellisel moel olla ettevõtte seadmete tegevuse ning olekuga kursis ning algas järsk ja kiire keskhaldussüsteemide juurutamine (MarketsandMarkets, 2022).

3.1 Mobile Device Management (MDM)

Apple’i algusaastatel töötasid kõik OS X arvutid täiesti eraldatuna teistest süsteemidest ning nende haldamine oli sisuliselt võimatu – see tõi kaasa aja möödudes Apple seadmete populaarsuse kadumise, sest Microsofti tooted suutsid pakkuda palju enamat nii kodukasutajatele kui ka ettevõtetele. Apple seadmeid kasutati varasemalt peamiselt koolides, sest seal tuli esile rohkem seadmete eeliseid kui puudusi. Mõne aja möödudes tutvustati turule toona uut ja innovatiivset seadet

– iPhone telefoni, mis andis suure tõuke seadmehalduse arendamiseks. 2010. aastal tutvustas Apple esmakordselt koos iOS 4 tulekuga ka MDM teenust, mis oli esialgu loodud vaid profiilide haldamiseks iOS seadmetel, lisaks profiilide haldamisele tutvustati esimeses väljalaskes ka kolme funktsiooni: määra asukoht, lukusta ja pühi. Peale seda muutus ettevõtetes ka suhtumine Apple seadmetesse ning IT-süsteemide administraatoritel tekkis lootus, et ühel päeval saab võimalikuks ka OS X seadmete keskne haldus (Edge & Trouton, 2019). Tänaseks on MDM teenust järjepidevalt arendatud ning iga uuendus toob kaasa suuri muutusi ja uusi võimalusi IT-administraatorite töös nii iOS kui ka macOS seadmetele (Joonis 5) (Edge & Trouton, 2019).

iOS versioon	Apple OS versioon	Aasta	Lisandunud featuurid
4	N/A	2010	Volume Purchase Program (VPP), Mobile Device Management (MDM), MDM macOS jaoks
5	10.7	2011	Üle õhu OS uuendused, Siri haldus, iCloud varunduse väljalülitamine
6	10.8	2012	APId kolmanda osapoole arendajatele, Managed Open In, Device Supervision
7	10.9	2013	TouchID haldus, Activation Lock bypass, Managed App config
8	10.10	2014	Device Enrollment Program, Apple Configuration enrollments
9	10.11	2015	Seadmepõhine VPP, B2B App Store, supervision reminders, rakenduste keelamine ning lubamine, avakuva kontroll, kiosk režiim/rakenduse lukustus
10	10.12	2016	Seadme taaskäivitamine, seadme sulgemine, Lost Mode, APFS
11	10.13	2017	Classroom 2.0 haldus, Managed FaceID haldus, AirPrint. Seadmete lisamine DEP'i, QR koodil põhinev liidestamine MDMiga, kasutaja luba MDM seadistuses Mac arvutiga
12	10.14	2018	Apple Business Manager, OAuth hallatud Exchange kontodele, hallatud tvOS rakenduse install, paroolilahtri automaatselt täitmise poliitikad
13	-	2019	Content Caching konfiguratsioon, Bluetooth haldus, autonoomne single app režiim, OS uuenduse edasi lükkamine, automaatne Active Directory sertifikaadi uuendamine

Joonis 5. MDM teenuse tähelepanuväärsemad uuendused läbi ajaloo (Edge & Trouton, 2019)

Lähtuvalt joonisel väljatoodust on võimalik väita, et suuremahulisi uuendusi on tõesti tehtud igal aastal. Seadmete keskhaldustarkvarasid on erinevaid ja neil kõigil on oma eelised ning puudused. Tuntuimad rakendused on: Amtel MDM, AppTrack, Codeproof, Kony, SimpleMDM, Miradore, Mosyle, Jamf, Intune (Edge & Trouton, 2019). Tänasel päeval on neist populaarseimateks ning üksteisele suurimateks konkurentideks Jamf ja Mosyle, viimase võttis kasutusele ka Ekspress Grupp. Apple seadmeid on võimalik ühendada ettevõttes kasutusel oleva MDM teenusega kolmel erineval viisil: kasutades Apple Business Manageri, Apple School Manageri või luues otse ühendus MDM serveriga. Meediakontsernis on kasutusel Apple Business Manager rakendus ning MDM teenus, mida kasutatakse peamiselt järgmisteks toiminguteks:

- Uute seadmete sidumiseks ettevõttega ning nende seadistamine.

- Profiilide rakendamine – võib võrrelda Windows süsteemides GPO rakendamisega.
- Operatsioonisüsteemide uuendused, versioonivahetused ja nende haldus.
- Kolmandate osapoolte rakenduste installeerimine ja nende uuendamine.
- Kasutajatele tarkvarakataloogi (*Self-Service*) pakkumine.

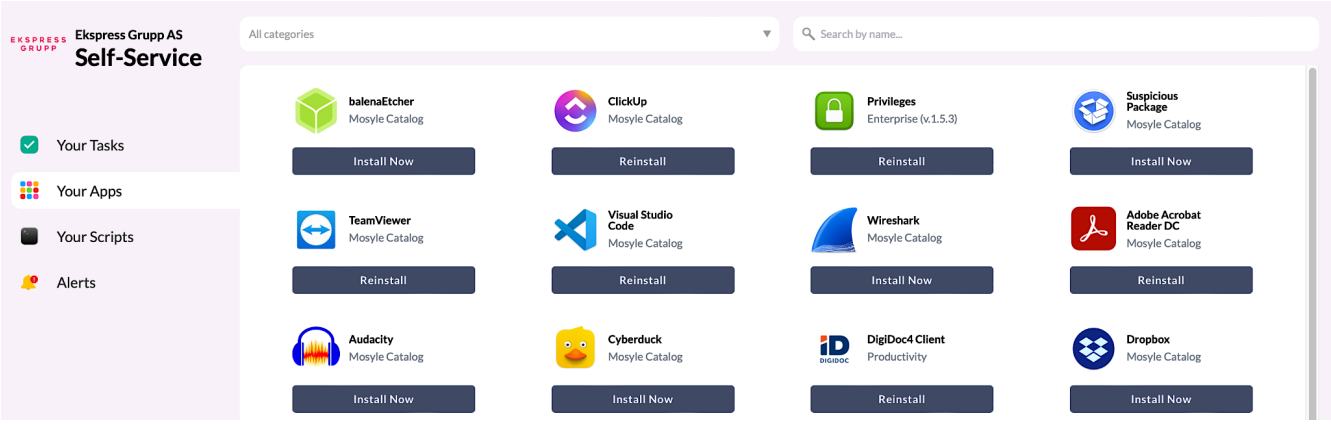
3.2 Apple Business Manager (ABM)

2018. aastal sai avalikkusele kättesaadavaks Apple Business Manageri teenus ning samal aastal valmis Apple'i ja Telia Eesti koostöös ka Eesti ettevõtetele pakutav Apple Businessi lahendus, mis muutis äriklientide elu tunduvalt mugavamaks. Apple Business Manager on teenus, mis on mõeldud Apple'i seadmeid kasutatavatele ettevõtetele. „Selle abil pääsevad ettevõtete IT-administraatorid organisatsioonide süsteemidesse, saavad kasutada seadmete üldjuurutust (*deploy*) ning osta vajalikul hulgal tarkvaralitsentse" (Valge Klaar, 2018).

Eestis oli Apple Business Manageri teenuse üks esimesi kasutajaid tarkvara arendav ettevõte Pipedrive, mille tehnikapark koosnes juba 2018. aastal 93% ulatuses Apple'i toodetest. Eelnevalt seadistati uusi seadmeid käsitsi, mis kulutas kallist tööaega ning töötajad ei saanud süvenenult keskenduda enda põhitegevustele. Rain Kõrgmaa mainis intervjuus, et tänu Apple Business Manageri ja MDM teenusele sujub uute seadmete paigaldus ja seadistamine tunduvalt kiiremini ja mugavamalt, sest IT-tehnikud ei pea süsteemi ega vajalikku tarkvara igale arvutikasutajale individuaalselt installima (Kõrgmaa, 2021).

Kõrgmaa väitis, et seadmejuhtimise teenus annab ettevõtte andmetele suurema turvalisuse ning ta soovitab Apple Business Manageri kõigile, kelle seadmepargis leidub Apple'i tooteid (Kõrgmaa, 2021).

Läbi Apple Business Manageri teenuse lingitakse valitud seadmed ettevõtte MDM serveriga (Mosyle Business), mis loob võimaluse kasutada VPP (*Apple Volume Purchase Program*) programmi, läbi mille saab osta App Store's olevate rakenduste litsentse – võimalik on valida kasutajapõhiste ning masinapõhiste litsentside vahel. Ekspress Grupis kasutatakse masinapõhist tarkvara litsentseerimist. VPP programm ilmus App Store'is saadavale 2010. aastal ning lahendas ettevõtete rakenduste litsentside hulgi ostmise probleemi (Edge & Trouton, 2019). Litsentside „ostmine" on võimalik ka tasuta rakendustele, selleks, et saaks neid lisada arvutite keskhalduses olevasse iseteeninduskeskkonda (*Self-Service*) – nii pole kasutajatel rakenduste allalaadimiseks vaja siseneda enda Apple ID kontoga App Store'i ega pole tarvis ka administraatori autentimist. Joonisel 6 (lk 19) on võimalik tutvuda *Self-Service* rakendusega.



Joonis 6. Seadmetes olev keskselt hallatav tarkvarakataloog *(Self-Service)*

Self-Service rakendusse on lisatud mitmeid erinevaid tarkvarasid. Joonisel välja toodud rakendus nimega Privileges on kasutusel IT-osakonnas peamiselt arendajate seadmetes – rakendus annab käivitamisel mõneks minutiks sisselogitud kasutajale administreerivad õigused.

3.3 Mosyle Business haldusrakenduse ülevaade

Ettevõttes on kasutustel Apple tööjaamade haldamiseks pilvepõhine Mosyle Business teenus, mis on loodud 2012. aastal Brasiilias Alcyr Araujo poolt ning on tänaseks kogunud palju populaarsust. Viimase kolme aasta jooksul on ettevõte hüppeliselt kasvanud ning rakendust kasutab rahvusvaheliselt tänaseks juba üle 32 000 organisatsiooni, millega hallatakse sadu tuhandeid Apple'i seadmeid.

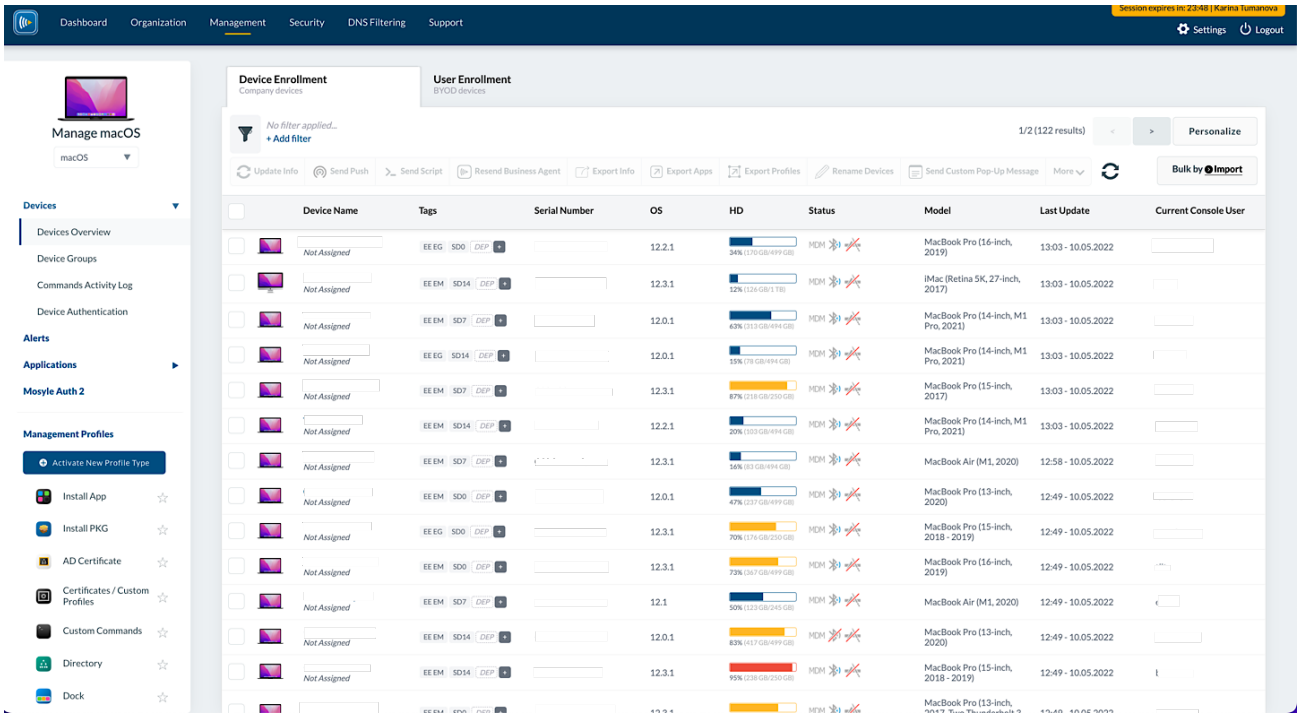
Mosyle Business on automatiseeritud keskhaldusrakendus, kuhu on täielikult integreeritud viis erinevat teenust (Mitchell, 2022):

- „Lummav" seadmete haldus *(Enchanted Device Management)* – Täielik MDM teenus macOS, iOS ning tvOS seadmetele, null-puudutus (*zero-touch*) seadmekonfigureerimine, tugi jagatud seadmetele, BYOD tugi, integratsioon Google, Microsoft Azure, Active Directory ning paljude teiste teenustega.
- Endpoint Security – 24/7 seadmeturve olenemata seadme asukohast, viimaste turvauuenduste olemasolu tagamine. Lahendus pakub ka antiviirust, pahavara tuvastamist, seadme puhastamist ning võimaldab kasutada Admin On-Demand teenust.
- Interneti privaatsus ning turvalisus *(Internet Privacy & Security)* – pakub krüpteeritud DNS-funktsiooni, mis automatiseerib veebi filtreerimist ning krüpteerimist.

- Identiteedihaldus *(Identity Management)* – ühendab Single Sign On (SSO) funktsionaalsuse kaheastmelise autentimisega, et luua kõrgeim turvalisus. Antud lahendus sunnib ettevõttes kasutada standardiseeritud seadmetesse sisselogimist ning toetab Okta, Ping Identity, Microsoft 365 ning Google Workspace teenuseid.
- Rakenduste haldus *(Application Management)* – Võimaldab ettevõtetel kaugelt installeerida, uuendada ning hallata Apple seadmetes olevaid rakendusi olenemata sellest, kas rakendus on olemas Apple App Store's või mitte.

Nii on loodud üks terviklik lahendus, mis pakub ettevõtetele kõiki võimalusi enda seadmete seadistamiseks, haldamiseks ning kaitsmiseks kasutades ühte rakendust (Mosyle Corporation, 2022). Mosyle Business peamisteks konkurentideks on Jamf Now (suunatud väikeettevõtetele) ning Jamf Pro (suunatud suurkorporatsioonidele). Mosyle Businessi eeliseks Jamf rakenduse ees on peamiselt tema taskukohasus, professionaalne kasutajatugi ning kiire teenuse edasiarendamine – klientide pöördumistele reageeritakse kiirelt, tähelepanekuid võetakse kuulda ning tihti saavad soovid ka täidetud (Evans, 2021). Autori poolt loodud pöördumistele on samuti alati kiirelt vastatud ning mure lahendatud.

Ekspress Grupis juurutati Mosyle Business rakendus 2020. aastal eesmärgiga rakendada sarnaselt Windows tööjaamadele ettevõttesiseseid turvapoliitikaid ning lihtsustamaks IT-tehnikute tööd uute Apple seadmete seadistamisel. Haldusrakendus annab selge ülevaate hetkel süsteemis olevatest masinatest ning nende seisukorrast, kes on arvutisse sisse logitud, mis operatsioonisüsteemi seade kasutab, kui palju on kettal ruumi, kas on esinenud töökindluses tõrkeid ja palju muudki. Nii on võimalik ennatlikult kasutajate seadmetega seonduvaid probleeme ennetada, märgata ning pakkuda kiirelt abi. Joonisel 7 (lk 21) on kuvatõmmis Mosyle Business rakendusest.



Joonis 7. Keskhalduses olevate seadmete ülevaade Mosyle Business rakenduses

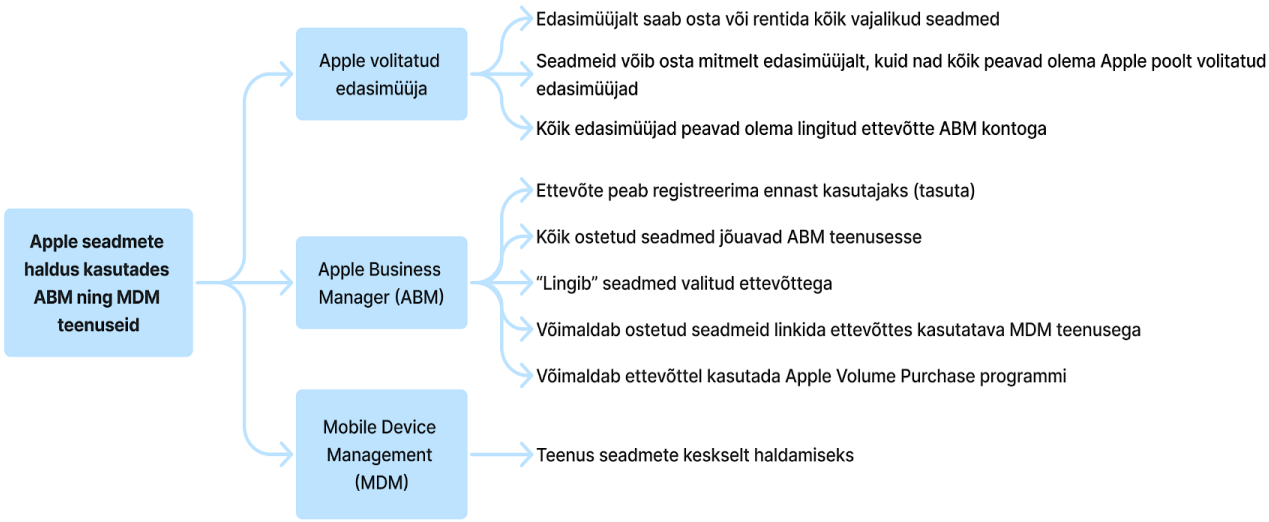
Joonisel kujutatud rakenduse pealehel on võimalik näha: seadme nime ja seerianumbrit, seadme operatsioonisüsteemi versiooni, ketta mahu täituvust, seadme staatust, seadme mudeli nime, sisselogitud kasutaja kasutajanime ning aega, millal seadmega uuendatud teabe saamiseks viimati süsteemis ühendust on võetud.

Kontsernil on mitmeid tütarettevõtteid, kus on kasutusel erinevad Windowsi domeenid. Hetkel lisatakse keskhaldussüsteemi lisamise protsessi ajal arvutid kindla ettevõtte Windows domeeni ning hetkel puudub võimekus valida mitme domeeni vahel. Loodud süsteemi vajadus on aga ajas muutunud ning see takistab teiste ettevõtete seadmete keskhaldusesse üleviimist. Selleks, et oleks võimalik teiste ettevõtete Apple tööjaamad liidestada keskhaldusega on tarvis luua uus funktsionaalsus, mis võimaldaks kasutajatel ennast macOS seadmetes erinevatest domeenidest autentida.

3.4 Seadmete keskhaldussüsteemi liidestamise protsessi kirjeldus tütarettevõtte Delfi Meedia näitel

Selleks, et Apple seadmeid oleks tehniliselt üldse võimalik liidestada kasutusel oleva keskhaldustarkvaraga (kasutades Apple Business Manageri) on tähtis, et nad kõik oleks soetatud Apple volitatud edasimüüjalt. Ühel ettevõttel võib olla ka mitu edasimüüjat, kelle kaudu soetatakse tehnikat, kuid nad kõik peavad olema sel juhul lingitud ettevõtte Apple Business Manager (ABM)

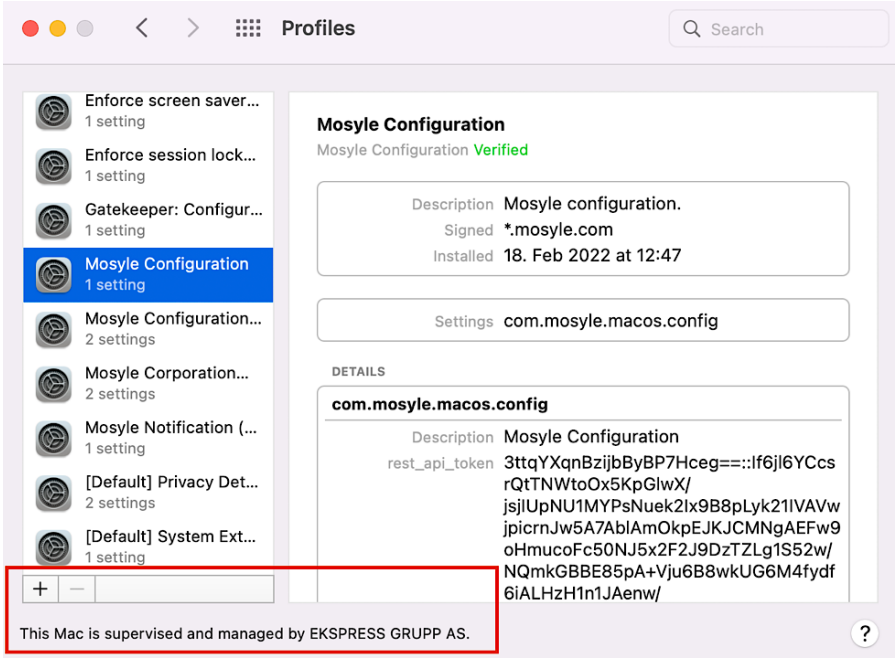
kontoga. ABM konto loomine ettevõttele on tasuta, kõik ostetud seadmed jõuavad ABM teenusesse, mis lingib need valitud ettevõttega. ABM teenus võimaldab seejärel ostetud seadmed linkida ettevõttes kasutatava MDM teenusega. Joonisel 8 on kirjeldatud Apple seadmete haldus kasutades ABM ning MDM teenuseid.



Joonis 8. Apple seadmete haldus kasutades ABM ning MDM teenuseid

Kui uued ostetud seadmed on lingitud MDM teenusega, on nad juba keskse halduse all ning arvuti esmasel käivitamisel kuvatakse nähtavale ettevõtte konfiguratsiooni aken teavitusega, et arvuti kuulub Ekspress Grupile. Antud etapis installeeritakse arvutisse erinevaid haldusprofiile. Haldusprofiilid on XML failid, mis panevad seadme kindlal viisil käituma ning konfigureerivad arvuti seadeid (Edge & Trouton, 2019). Haldusprofiile on võimalik luua kasutades Mosyle Business teenust, kuid vahest tuleb luua konfiguratsiooniprofiilid käsitsi – sellisel juhul kasutatakse ettevõttes iMazing Profile Editor rakendust, mille kasutusmugavuse tõttu on uusi profiile lihtne konfigureerida. Kui profiilid on taustal installeeritud peab IT-administraator lisama arvuti vajalikesse seadmegruppidesse (üldiselt osakonna põhiselt) ning seejärel saab kasutaja arvutisse juba sisse logida.

Ekspress Grupis määratakse profiilidega näiteks järgmised seaded: kasutaja ei saa „Erase Mac“ valikuga arvuti operatsioonisüsteemi kustutada, AirDrop on kasutamiseks keelatud, arvutisse saab rakendusi installeerida vaid App Store’st, tarkvarakataloogist või identifitseeritud arendajatelt, teostusüksuse osakonna arvutitel on eriline doki vaade jne. Halduses olevatel masinatel on keelatud kasutajatel profiilide eemaldamine või muutmine (Joonis 9, lk 23).



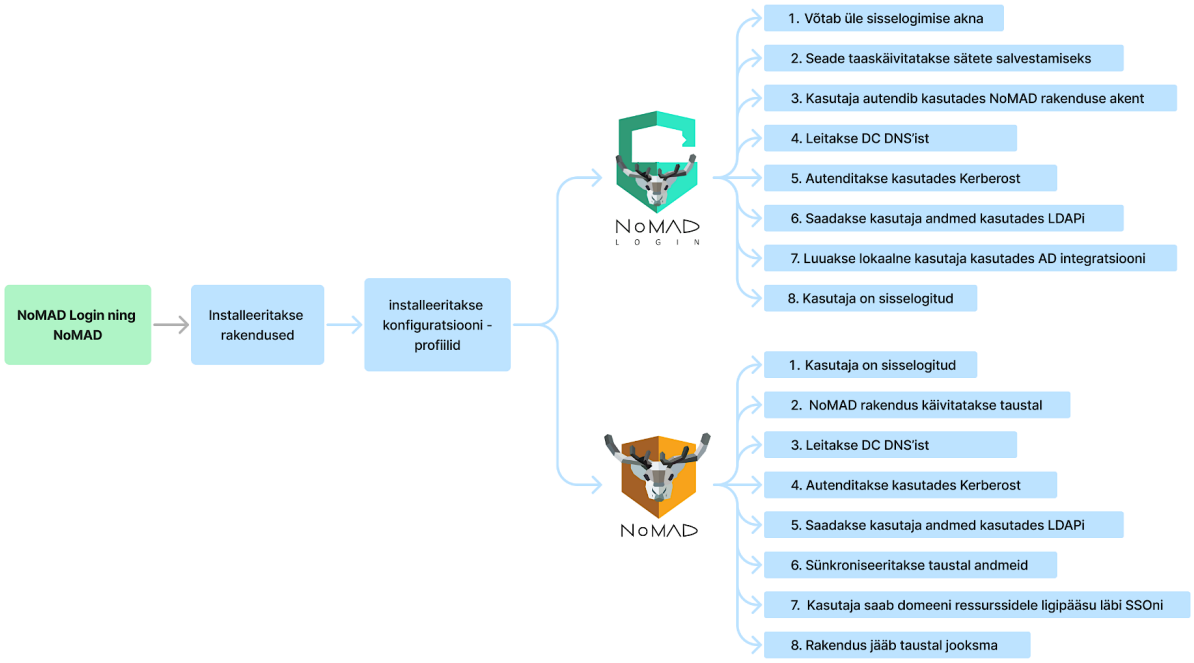
Joonis 9. Installeeritud profiilide nimekiri tööjaamas

Joonisel on kuvatud kasutajatele nähtav teavitus „*This Mac is supervised and managed by EKSPRESS GRUPP AS*“, mis viitab sellele, et kasutaja ei saa profiile ise eemaldada või muuta.

3.4.1 Seadmete liidestamine domeeniga

Hetkel toimub seadmete domeeni liidestamine kasutades konfiguratsiooniprofiili, mis installeeritakse arvuti seadistamise käigus. Antud profiiliga lisatakse seade domeeni, määratakse Active Directorys (edaspidi AD) seadmele nimi, määratakse grupid, mille kasutajatel on õigus ennast arvutis lokaalse administraatorina autentida ning määratakse kui tihti masina AD parooli muudetakse. Sisevõrku autentimiseks kasutab tööjaam kasutaja AD sisselogimise andmeid. Keskhalduses olevasse arvutisse sisselogimiseks kasutavad töötajad enda AD kasutajanime ning parooli.

Selleks, et see oleks võimalik, kasutatakse kahte rakendust: NoMAD Login ning NoMAD. Joonis 10 (lk 24) tutvustab NoMAD ning NoMAD Login rakenduste tööpõhimõtteid.

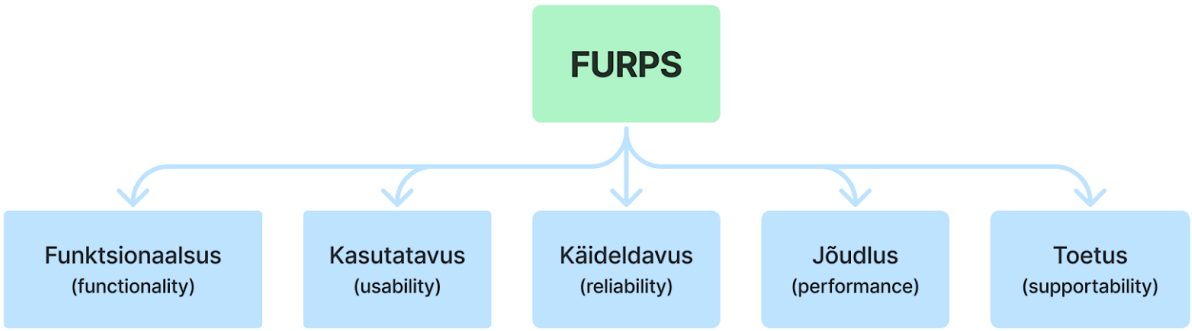


Joonis 10. NoMAD ning NoMAD Login rakenduste tööpõhimõtted

NoMAD Login (kontrollib kasutaja sisselogimise andmeid ning loob lokaalse kasutaja) ning NoMAD (käivitub peale kasutaja sisselogimist, võimaldab kasutajal pääseda ligi domeenis olevatele ressurssidele ning hoolitseb selle eest, et lokaalse- ning AD kasutaja paroolid oleksid sünkroniseeritud). Antud rakendused on Joel Rennich poolt loodud ning nad on vabavaralised – ehk tarkvara, mida saab ilma piiranguteta kasutada (Orchard & Grove Inc., 2022).

4 LISATAVA FUNKTSIONAALSUSE NÕUETE KAARDISTAMINE JA PRIORITISEERIMINE (*TO-BE*)

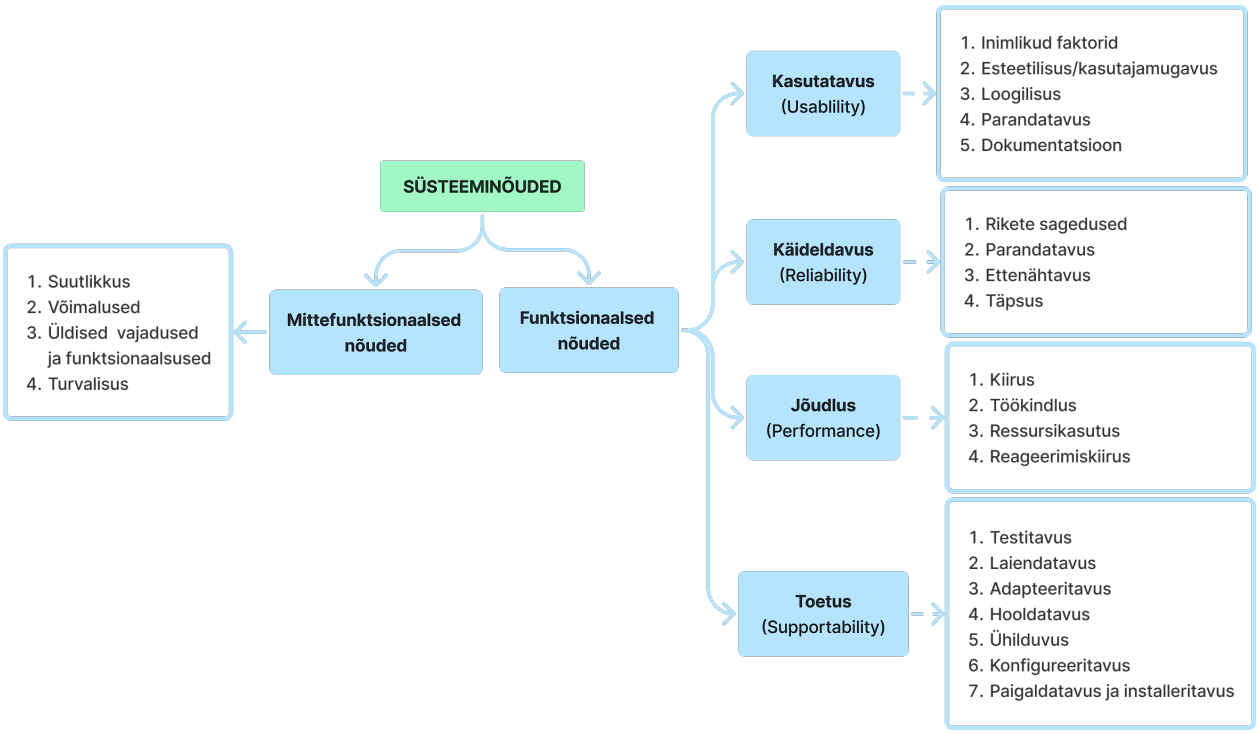
Uue tarkvara või funktsionaalsuse arendamine ning loomine algab eeluuringust, millele järgneb vajalike nõuete kirjapanemine. Süsteeminõudeid on võimalik kirjeldada kasutades erinevaid raamistikke. Antud töös kasutas autor lisatava funktsionaalsuse nõuete kirjeldamiseks ning klassifitseerimiseks tarkvaraarenduses laialtlevinud juurutusmetoodikat FURPS. Antud metoodikat tutvustati esmakordselt 1987. aastal Robert Grady ning Deborah Caswell poolt. FURPS metoodika tugineb viiele peamisele kategooriale: funktsionaalsus (*functionality*), kasutatavus *(usability),* käideldavus *(reliablility),* jõudlus *(performance)* ning toetus *(supportability)* (Adams, 2015) (Joonis 11).



Joonis 11. FURPS metoodika kategooriad (funktsionaalsus, kasutatavus, käideldavus, jõudlus, toetus)

Kõik nõuded saab klassifitseerida kaheks: funktsionaalsed- ning mittefunktsionaalsed nõuded. Funktsionaalsed nõuded vastavad enamjaolt küsimusele „Mida peab antud tarkvara tegema“ ja on kirjeldatud funktsionaalsuse kategoorias. Mittefunktsionaalsed nõuded vastavad küsimusele „Kuidas peab antud tarkvara neid funktsioone täitma?“ ning need on kirjeldatud kasutatavuse, käideldavuse, jõudluse ning toetuse kategooriates (Tepandi, 2022).

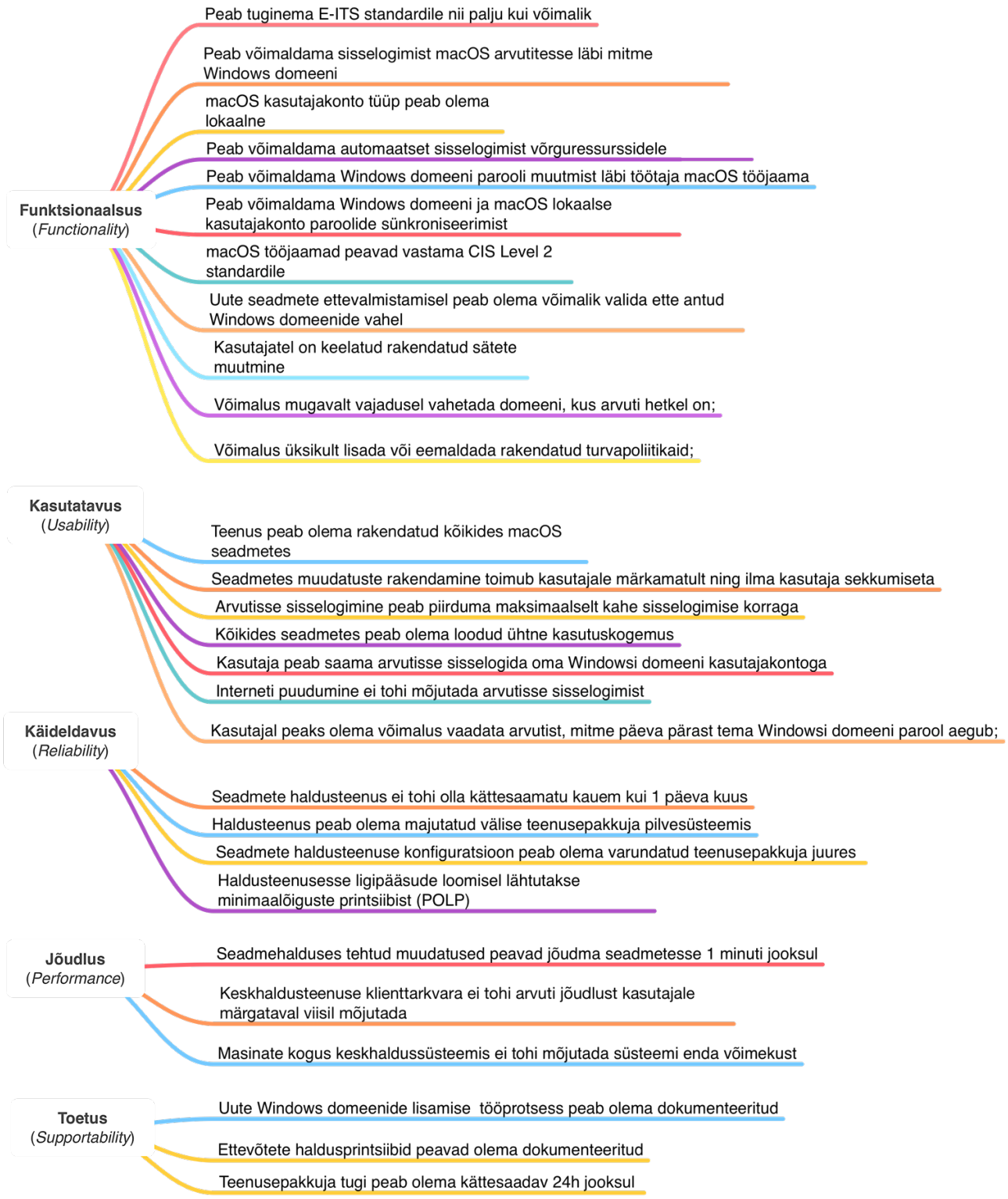
Funktsionaalsete nõute kategoorias keskendutakse konkreetsetele funktsionaalsustele ning võimalustele, mida loodav rakendus peab tegema. Järgneval joonisel (Joonis 12, lk 26) on välja toodud FURPS metoodika peamised kategooriad ning sinna kuuluvad atribuudid.



Joonis 12. FURPS mudeli kategooriad ning atribuudid (Adams, 2015)

Kasutatavuse kategooria kirjeldab, kes toodet kasutab ja kuidas seda kasutatakse. Süsteemi käideldavus tagatakse kirjeldades rikete sageduste esinemise võimalust ning süsteemi parandatavust ja täpsust. Jõudluse tagamiseks kirjeldatakse võimalikult täpselt süsteemi töökindlus, kiirus, ressursikasutus ning reageerimiskiirus. Toetuse all peetakse silmas süsteemi hilisemat hooldamist ning tuge.

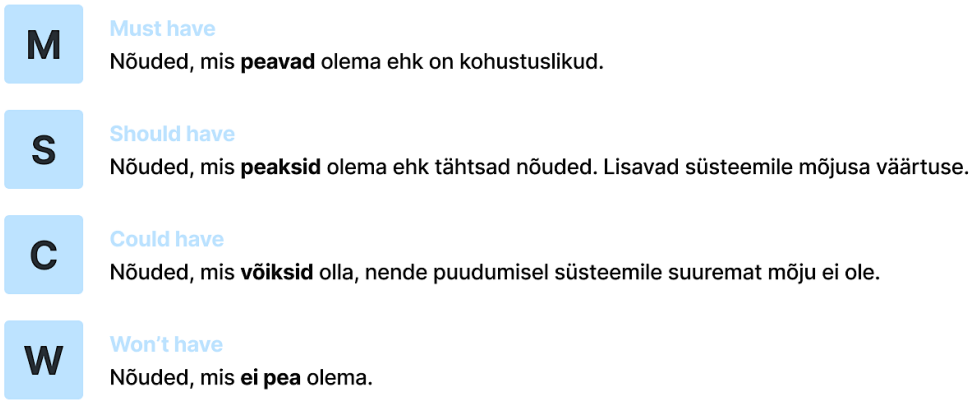
Koos Ekspress Grupi IT süsteemiadministraatoriga kaardistati 09. märtsil 2022. aastal toimunud koosolekul lisatava funktsionaalsuse süsteeminõuded ning koostati joonis kasutades MindNode rakendust (Joonis 13, lk 27). Kirjeldatud FURPS nõuetega on võimalik tutvuda Lisas 4 (lk 56).



Joonis 13. Kaardistatud süsteeminõuded kasutades FURPS metoodikat

4.1 Nõuete prioritiseerimise teoreetilised lähtekohad

Lisatava funktsionaalsuse nõuete prioritiseerimiseks kasutati MoSCoW prioritiseerimise meetodit. „Mõiste MoSCoW on akronüüm prioritiseerimise kategooriatest *(Must have, Should have, Could have, Won't have)*“ (Kehtna Kutsehariduskeskus, 2018). Kokkuvõttes on kõik süsteemile seatud nõuded olulised, kuid aja paremaks planeerimiseks ning ettearvamatuste korral korrektseks tegutsemiseks on vaja kõik nõuded siiski eelnevalt prioritiseerida – ajapuuduse või probleemide esinemisel jäetakse vähemolulised nõuded esialgu kõrvale ning keskendutakse nendele hiljem (Kehtna Kutsehariduskeskus, 2018). MoSCoW meetodi nime tähenduse võib lahti seletada järgmiselt: *must have* ehk nõuded, mis peavad olema, funktsiooni või süsteemi omadused, mis on kohustuslikud; *should have* ehk tähtsad nõuded, mis ei ole niivõrd olulised kuid siiski lisavad süsteemile mõjusa väärtuse; *could have* ehk nõuded, mis võiksid olla, kuid nende puudumisel süsteemile suuremat mõju ei ole ning *won't have* ehk nõuded, mis ei ole hetke ajajooksul prioriteediks (Güzelsevdi, 2021). Joonisel 14 on kirjeldatud MoSCoW meetodi tähendus.



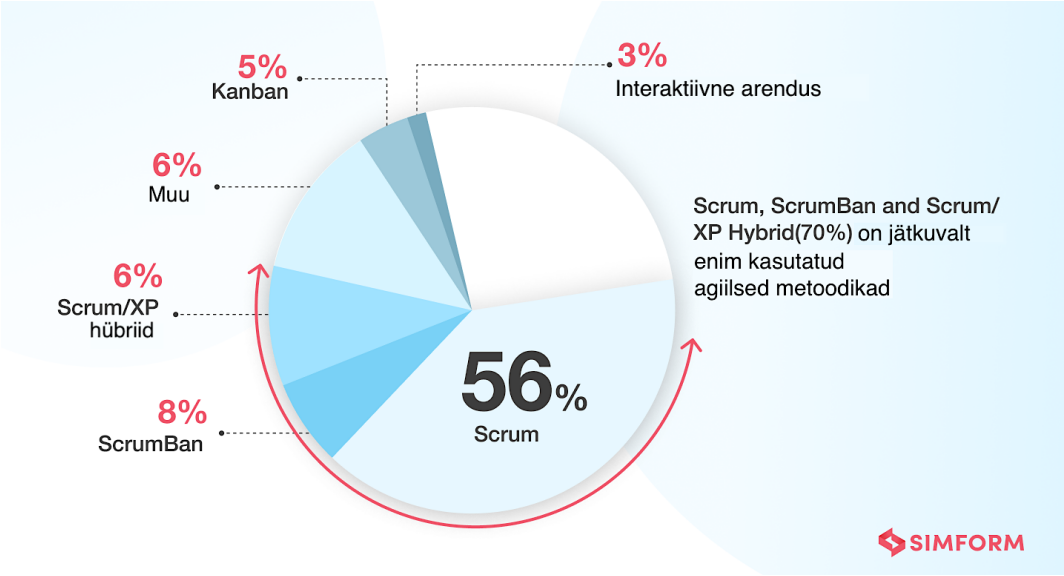
Joonis 14. MoSCoW meetodi tähendus (Güzelsevdi, 2021)

MoSCoW meetod on üpriski lihtne ning konkreetne. Sellisel viisil prioritiseerimine aitab paremini keskenduda projekti tähtsatele eesmärkidele ning töö fookus ja skoop püsib paigas – nii vähendatakse ka töö käigus tekkivaid vigu. Prioriteedid määrati 23. märtsil 2022 toimunud koosolekul, kus osales töö autor, IT kasutajatoe juht ning IT süsteemide administraator. Koosolekul jaotati varasemalt kirjeldatud nõuded nelja gruppi: peavad olema, peaksid olema, võiksid olla ning nõuded, mida hetke ajajooksul ei pea olema. Kohustuslikke nõudeid (*must have*) kirjeldati kokku 20, nõudeid, mis peaksid olema (*should have*) tuli kokku 5. Nõudeid, mis võiksid olla (*could have*) tuli kokku kaks ning nõudeid, mida ei pea olema tuli kokku 1. MoSCoW meetodi järgi nõuete ülevaade on tabelina nähtaval Lisas 5 (lk 57).

5 LISATAVA FUNKTSIONAALSUSE LOOMISE, TESTIMISE JA JUURUTAMISE TEOREETILISED JA METOODILISED LÄHTEKOHAD

Viimaste aastakümnete jooksul on ettevõtted hoogsalt hakanud kasutama agiilseid arendusmeetodeid ehk välearendust, et pidada sammu erinevate kiirete muutuste ning kasvava nõudlusega. Esimesed tähelepanekud agiilsetest praktikatest levisid juba 1980-1990 aastatel kuid nendest olid kuulnud vaid vähesed. 2001. aasta talvel kohtusid 17 agiilse tarkvaraarenduse entusiasti Utah's Snowbirdi suusakuurordis, et arutleda ja defineerida uut lähenemist tarkvara arendamisele. Senised viisid tundusid neile ebamõistlikud ning rahaliselt liiga kallid. Kohtumise käigus defineeriti 4 väärtust ning 12 põhiprintsiipi, millele agiilne arendus keskendub ning see dokument sai nime agiilse tarkvaraarenduse manifest (*MoSCoW Prioritization*, s.a.).

Tänaseks kasutavad ligikaudu pooled agiilseid praktikaid kasutavad ettevõtted Scrum raamistikku (Viscardi, 2013) (Joonis 15).

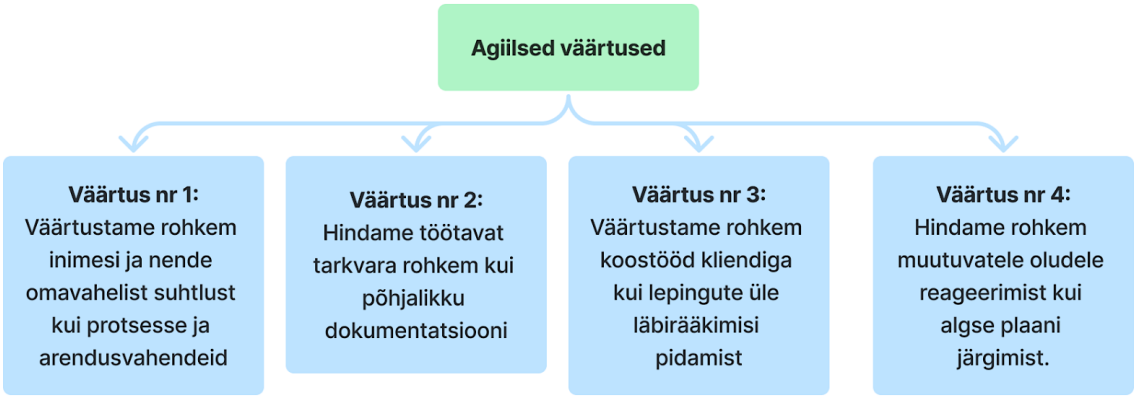


Joonis 15. 56% ettevõtetest eelistavad Scrum raamistikku (Akiwatkar, 2022)

Levinud on vale arusaam, et Scrum on eraldiseisev arendusmeetod – tegelikult on tegemist agiilse lähenemisviisiga ehk raamistikuga, mis põhineb reeglite koosmõjul, distsipliinil, isiklikul vastutusel, ühisel mõtlemisel, üksteise abistamisel ning teadmiste mitte kasutamisel isikliku hiilguse nimel (Gloger et al., 2013). Scrum raamistik toetub neljale agiilse manifesti väärtusele (Joonis 16, lk 30),

kuigi lausete teises pooles kirjeldatu on samuti tähtis, keskendutakse lause esimeses osas kirjapandule märgatavalt rohkem:

- Väärtustame rohkem inimesi ja nende omavahelist suhtlust kui protsesse ja arendusvahendeid.
- Hindame töötavat tarkvara rohkem kui põhjalikku dokumentatsiooni.
- Väärtustame rohkem koostööd kliendiga kui lepingute üle läbirääkimisi pidamist.
- Hindame rohkem muutuvatele oludele reageerimist kui algse plaani järgimist (*Manifesto for Agile Software Development*, 2001).



Joonis 16. Agiilsed väärtused

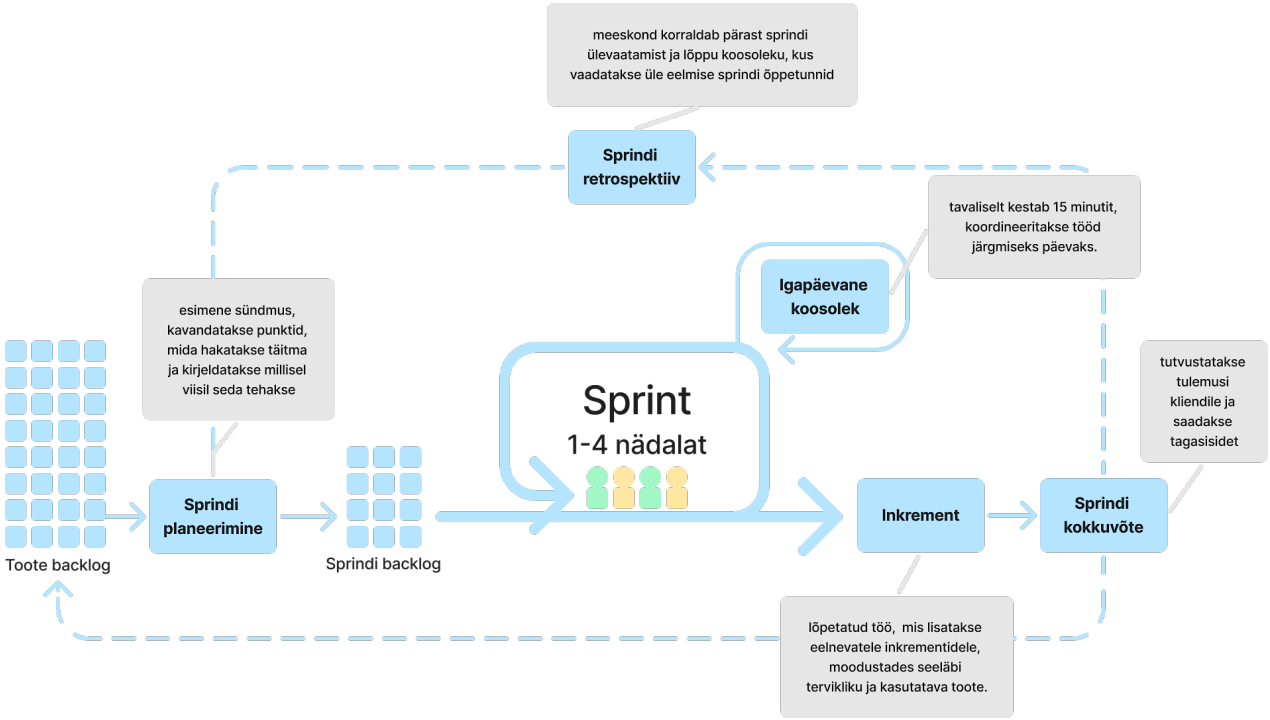
Lisaks neljale väärtusele defineerib agiilset arendust ja Scrum raamistikku ka 12 põhiprintsiipi:

- Kõige tähtsam on tagada kliendi rahulolu.
- Mõistame ning aktsepteerime muutusi ka arenduse lõppfaasis.
- Tarnime funktsionaalsusi/tarkvara iga paari nädala kuni paari kuu tagant.
- Ala eksperdid ja arendajad töötavad projekti käigus koos igapäevaselt.
- Edu aluseks on motiveeritud tiimiliikmed, vajalik on meeldiv ja turvaline töökeskkond.
- Kõige tulemuslikum suhtlusviis on näost-näkku vestlemine.
- Edu mõõdupuuks on funktsioneeriv tarkvara.
- Agiilse tarkvaraarendusega soodustame jätkusuutliku arendust.
- Hoiame pidevat tähelepanu tehnilistel detailidel ja heal disainil, nii tagame tarkvaraarenduse kiiruse ja paindlikkuse.
- Jätame ebavajaliku töö tegemata.
- Iseorganiseeruvad meeskonnad suudavad välja töödelda parimad arhitektuurilised lahendused, nõuded ja disaini.

- Regulaarsete intervallidega otsitakse võimalusi meeskonna muutmiseks tõhusamaks (Gloger et al., 2013b).

Scrumi raamistikus on kolm rolli: tooteomanik *(Product Owner)*, Scrum meister ehk juht *(Scrum Master)* ja arenduse meeskond *(Scrum Team)*. Tooteomanik peab läbirääkimisi kliendiga, määratleb arendatava toote omadused ja nõuded, loob nendest nimekirja ning lisab seejärel ülesanded *backlogi*. Scrum meister hoolitseb selle eest, et arendusmeeskond tegutseks Scrumi põhimõtete ja väärtuste kohaselt ning et välised tegurid ei saaks meeskonda mõjutada. Arendusmeeskond vastutab tarkvara arendamise eest, ühe meeskonna suuruseks on üldjuhul alla 7 inimese (Petuhhov (TLÜ), 2023). Projektis täitis autor mitut rolli – oli projektijuht, tegeles uue funktsionaalsuse arendamisega, aitas määratleda arendatava toote omadused ja nõuded, prioritiseeris need koostöös tiimikaaslasega, koostas dokumentatsiooni.

Scrum koosneb viiest sündmusest: sprint, sprindi planeerimine, igapäevane koosolek, sprindi kokkuvõte ning sprindi retrospektiiv ehk tagasivaade. Joonisel 17 on kirjeldatud Scrum raamistik.



Joonis 17. Scrum raamistik

Sprint ehk iteratsioon algab koosolekust, kus planeeritakse sprindi vältel kõik tehtavad tööd, sellele järgnevad igapäevased kuni 15 minutilised koosolekud, kus arutatakse, mida tehti eile, mida tehakse täna ning kas tööl on takistusi. Sprindi planeerimise aluseks on seni tegemata tööde loetelu ehk toote

backlog. Sprint kestab üldjuhul alates nädalast kuni kuuni, sprindi lõpus tehakse koosolek, kus tutvustatakse kliendile reaalset valmis tulemust ning seejärel korraldatakse meeskonnasisene sprindi retrospektiiv arutamaks, mis sprindis läks kehvasti või vastupidi hästi.

Projektide tulemuslikumaks juhtimiseks kasutavad meeskonnaliikmed ülesannete ja sprintide visualiseerimiseks Scrum tahvlit (Scrum *board*) – tahvlil on võimalik näha kõiki projektiga seotud ülesandeid ja nende hetkeseisu. Üldjuhul jaotatakse tahvel neljaks: "*backlog*" ehk tegemata tööd, "*to-do*" ehk tööd, mida on vaja hakata tegema, "*in progress*" ehk tegemisel ning "*done*" ehk tehtud ülesanded (Bottorff & Crail, s.a.).

Autori hinnangul sobib Scrum raamistik lõputöö käsitlemiseks paremini kui teised raamistikud, eelkõige seetõttu, et ta keskendub rohkem meeskonnatööle ning paindlikkusele, võimaldab erinevates etappides viia vajadusel sisse muudatusi ilma, et see oleks problemaatiline - nii on meil võimalik kiiresti reageerida erinevatele muutustele. Scrum on parem valik olukordades, kus projekti nõuded võivad jooksvalt muutuda, koskmudel sobib paremini arendustele, kus nõuded on kindlalt paigas ja kus on vaja tagada kvaliteet ja stabiilsus.

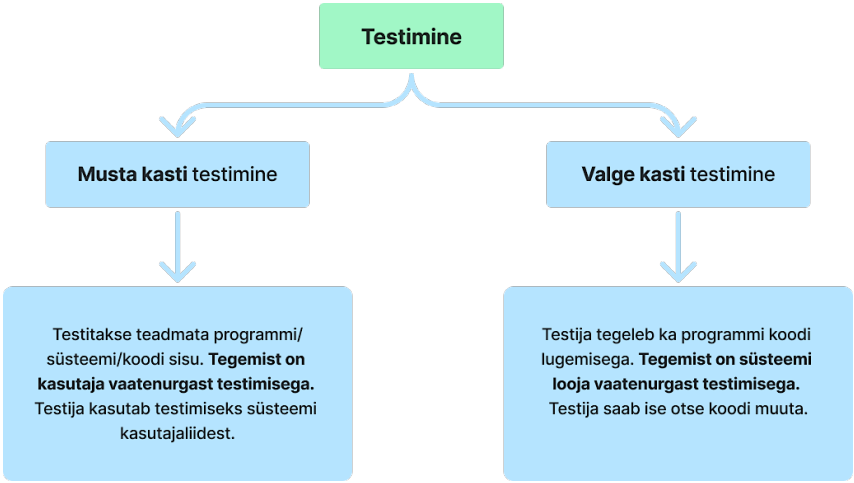
19. oktoobril 2022 lepiti korraldatud koosolekul kokku, et lisatava funktsionaalsuse loomiseks ning juurutamiseks kasutatakse Scrum raamistikku ja kõikide eelduste kohaselt teostatakse kolm sprinti. Sprintide toimumise ajad lepiti kokku järgnevalt:

1. I sprint toimus ajavahemikus 14.11.2022-18.11.2022.
2. II sprint toimus ajavahemikus 12.12.2022-16.12.2022.
3. III sprint toimus ajavahemikus 16.01.2023-20.01.2023.

5.1 Lisatava funktsionaalsuse testimine

Kõige levinumaks viisiks kontrollimaks, kas loodud tarkvara teeb kõike ettenähtut ja on saavutatud kõik kirjeldatud nõuded, on testimine (Tepandi, 2022). Testimise eesmärk on kinnitada, et loodud tarkvara või lahendus teeb täpselt seda, mis vaja. Testimist on laiemalt võimalik liigitada tuginedes testija vaatenurgale või sihtmärgile, testitava osa taseme alusel või tuginedes sellele, kas testimise läbiviijaks on inimene või rakendus. Liigitamist alustatakse jagades testimine tervikuna kaheks: musta kasti testimine ning valge kasti testimine (Joonis 18 , lk 33). Musta kasti testimine (*black box testing)* toimub kasutades kasutajaliidest ning ilma, et testija peaks süsteemist süvitsi aru saama või koodi mõistma. Valge kasti testimine *(white box testing)* eeldab testijalt teadmisi arenduse,

programmi ning koodi kohta – testija teeb vajadusel soovitud muudatused ise otse koodi muutes (Vorteil & Laanpere, 2023).



Joonis 18. Testimise liigitamine: musta kasti testimine ning valge kasti testimine

Seejärel on võimalik testimine omakorda liigitada tuginedes testimise sihtmärkidele, testimise eesmärgiks võib olla ka vaid ühe kindla sihtmärgi testimine, näiteks testitakse süsteemi turvalisust. Testimise peamiseid tüüpe on kokku kümme:

- Moodultestimine – testitakse konkreetset moodulit.
- Integratsioonitestimine – testitakse erinevate moodulite koostoimimist.
- Süsteemtestimine – testitakse süsteemi kui terviku toimimist.
- Regressioontestimine – igat tüüpi tarkvara testimine, veendumaks, et lisatud uuendus ei põhjusta uusi probleeme.
- Jõudlus- ja koormustestid – testitakse süsteemi tehnilisi nõudeid.
- Valideerimine – kinnitatakse, et tarkvara sobib kasutamiseks.
- Verifitseerimine – kinnitatakse, et iga tulem vastab nõuetele.
- Kasutatavuse testid – testitakse ja hinnatakse kasutusmugavust.
- Vastuvõtutest – viib läbi klient, hinnatakse tarkvara vastamist kõikidele nõuetele.
- Koodi läbivaatamine – inspekteeritakse koodi (Petuhhov, 2011).

Autori hinnangul on sobilik kasutada musta kasti testimise viisi, sest selline lähenemine ei eelda testijalt süvitsi teadmisi süsteemi toimimisest ning testimiseks kasutatakse kasutajaliidest - testitakse süsteemi funktsionaalsusi kui tervikut. Testijateks on autor ning funktsionaalsuse lõppkasutajad (IT tehnikud). Uue funktsionaalsuse testimiseks kasutatakse integratsioonitestmist, süsteemtestimist, regressioontestimist ja kasutatavuse testimist. Testimine toimub sprintide käigus ning lõpus.

6 LISATAVA FUNKTSIONAALSUSE LOOMINE, TESTIMINE NING IMPLEMENTEERIMINE KONTSERNIS

Vajadus funktsionaalsuse järele defineeriti juba 2022. aasta alguses, nimetatud aasta märtsikuus kirjeldati funktsionaalsuse nõuded ning prioritiseeriti need. Seejärel jäi projekt mõningateks kuudeks seisma, sest autor oli tervislikel põhjustel töölt eemal. Projekti juurde naasti 2022. aasta oktoobrikuus, kui 19. oktoobril korraldati koosolek ning lepiti kokku Scrum raamistiku kasutamine ning kolme sprindi teostamine. Koosolekul kirjeldati ka *backlogi* ülesanded.

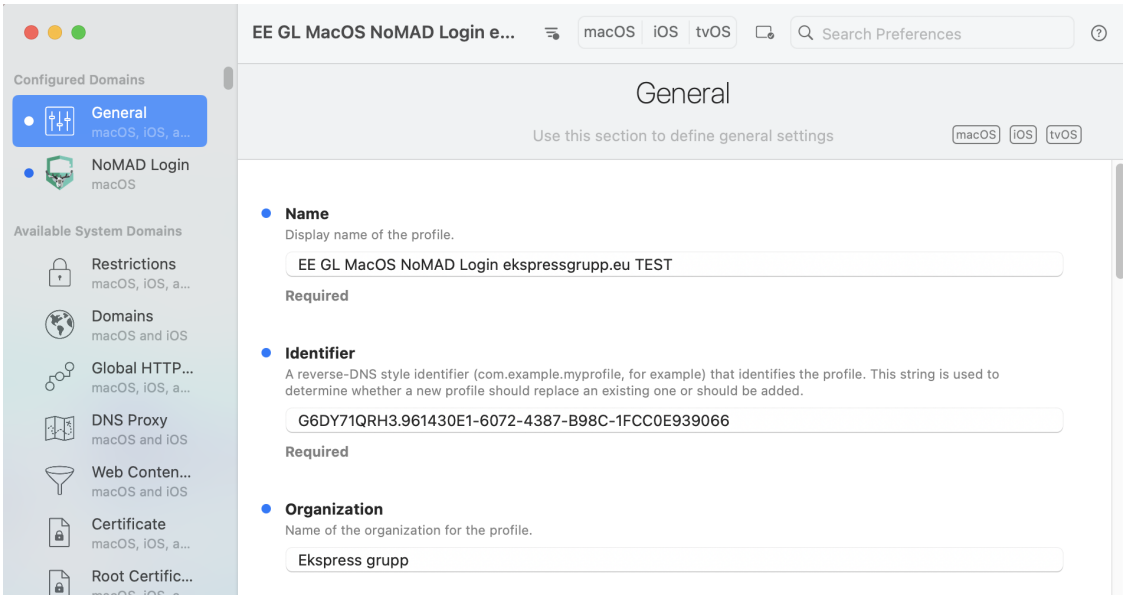
6.1 Ülevaade esimesest sprindist – uute konfiguratsiooniprofiilide loomine

I sprindi planeerimise ja sprindi *backlogi* kirjeldamise koosolek toimus päev hiljem, 20. oktoobril 2022, millest võtsid osa: IT süsteemide administraator, töö autor, ning IT kasutajatoe juht. Koosolekul kirjeldati seni tegemata tööde loetelu, esialgsed tegevused ning sõnastati esimese sprindi eesmärk – luua uue domeeni jaoks toimivad konfiguratsiooniprofiilid. Omavaheliseks suhtlemiseks loodi Slacki kanal (*channel*) ja projekti dokumenteerimiseks ning jooksvate tööde loetelu saamiseks loodi uus projekt ettevõttes kasutusel olevas Jira Service Management keskkonnas (*Scrum board*). Jira Service Management on arendusprojektide haldamise tarkvara, kus saab planeerida projekte ning määrata igale tiimiliikmele ülesandeid, Jira projektijuhtimise tööriist põhineb Scrum ning Kanban meetoditel (*Atlassiani tooted*, s.a.).

I sprint algas 14.11.2022 ning lõppes 18.11.2022. Sprindi jooksul toimusid hommikuti kuni 15 minutilised koosolekud arutamaks, kuidas ülesannetega on läinud ning kas on töö tegemisel takistusi. Eelnevalt koosolekul kokkulepitule oli esimese sprindi eesmärgiks luua uue domeeni jaoks *directory*, NoMAD ning NoMAD Login konfiguratsiooniprofiilid, millega on võimalik defineerida erinevaid seadistusi, eelistusi või piiranguid nii macOS kui ka iOS, iPadOS ja tvOS seadmetes luues seeläbi võimekuse liidestada uus domeen MDM teenusega. Loodud profiilid salvestati *.mobileconfig* failidena ning neid kasutati MDM teenuses.

Enne profiilide loomist lõi töö autor Active Directorys uue teenuskonto, millega on võimalik seadmeid teise domeeni lisada. Teenuskontode kasutamine on vajalik, et hoia eraldi isiklikud kasutajakontod ning IT süsteemide või teenuste toimimiseks vajalikud kontod – kokkuvõttes on see tunduvalt turvalisem valik.

Seejärel kasutas autor profiilide loomiseks ettevõttes kasutatavat iMazing Profile Editor rakendust. iMazing on DigiDNA nimelise ettevõtte poolt loodud tasuta rakendus, mis võimaldab luua, muuta ja allkirjastada Apple konfiguratsiooniprofiile. Rakendusel on lihtne ning arusaadav kasutajaliides ja seetõttu on rakendus ka väga laialt levinud (Leviatan, 2022). Joonisel 19 on kuvatõmmis iMazing Profile Editor rakendusest.



Joonis 19. iMazing Profile Editor rakendus

Kokku loodi ning testiti esimese sprindi jooksul kolm erinevat profiili: NoMAD, NoMAD Login ning *directory*. NoMAD profiili peamiseks ülesandeks on käivitada rakendus peale kasutaja sisselogimist, võimaldada kasutajal pääseda ligi domeenis olevatele ressurssidele ning rakendus hoolitseb selle eest, et lokaalse– ja AD kasutaja paroolid oleks sünkroonis. NoMAD Login profiil kontrollib kasutaja sisselogimise andmeid ning loob seejärel lokaalse kasutaja. NoMAD Login rakendus sünkroniseerib andmeid järgmistel põhimõtetel:

- Iga kord kui rakendus käivitatakse.
- Iga 15 minuti tagant.
- Iga kord kui arvutis vahetub võrguühendus.
- NoMAD ei sünkroniseeri andmeid kui domeen ei ole kättesaadav.

Directory profiiliga lisatakse seade domeeni ning määratakse seadmele Active Directorys nimi. Profiil määrab ka kindlad AD grupid (tööjaamade administraatorite grupp), mille kasutajad (IT tehnikud) saavad macOS seadmetes tegutseda administreerivate õigustega ning määrab kui tihti

kasutajate AD parool aegub. Peale nimetatud ülesannete täitmist testis autor konfiguratsiooniprofiilide toimimist.

I sprindi ülevaade ning retrospektiiv toimusid 22. novembril. Sprindi ülevaate käigus vaadati üle ülesanded, mis said tehtud ning tegevused, mida tuleb järgmisena tegema hakata. Retrospektiivi ajal arutati, mida järgmises sprindis saaks teha paremini. Kõik I sprinti määratud ülesanded said sooritatud ning sprindi eesmärk seeläbi täidetud. Sprindi ülevaade on kirjeldatud joonisel 20.

Nr	Eesmärk ning inkrement	Tehtavad ülesanded	Testimine	Sprindi jooksul täidetud nõuded
Sprint I 14.11.2022- 18.11.2022	Luua uue domeeni jaoks konfiguratsiooni-profiilid. **Inkrement** - toimivad konfiguratsiooniprofiilid.	1. Teenuskonto loomine seadmete lisamiseks domeeni; 2. NoMad konfiguratsiooniprofiili loomine 3. NoMad Login konfiguratsiooniprofiili loomine 4. Directory konfiguratsiooniprofiilide loomine teisele domeenile 5. Loodud profiilide testimine.	1. Integratsiooni-testimine; 2. Regressioon-testimine.	1. MacOS konto tüüp peab olema lokaalne; 2. Windows domeeni ja macOS tööjaama paroolide sünkroniseerimine; 3. Interneti puudumine ei tohi mõjutada arvutisse sisselogimist; 4. Haldusteenus peab olema majutatud välise teenusepakkuja pilvesüsteemis; 5. Haldusteenusesse ligipääsude loomisel lähtutakse minimaalõiguste printsiibist (POLP); 6. Masinate kogus süsteemis ei tohi mõjutada süsteemi enda võimekust; 7. Windows domeeni parooli muutmine peab olema võimalik läbi macOS tööjaama; 8. Kasutajal võimalus vaadata arvutist, mitme päeva pärast tema Windowsi domeeni parool aegub.

Joonis 20. Esimese sprindi ülevaade

Esimese sprindi tulemusel valmisid toimivad konfiguratsiooniprofiilid, mis võimaldavad lisada macOS seadet teise domeeni ning vastavalt joonisel kirjeldatule täideti sprindi jooksul 8 nõuet.

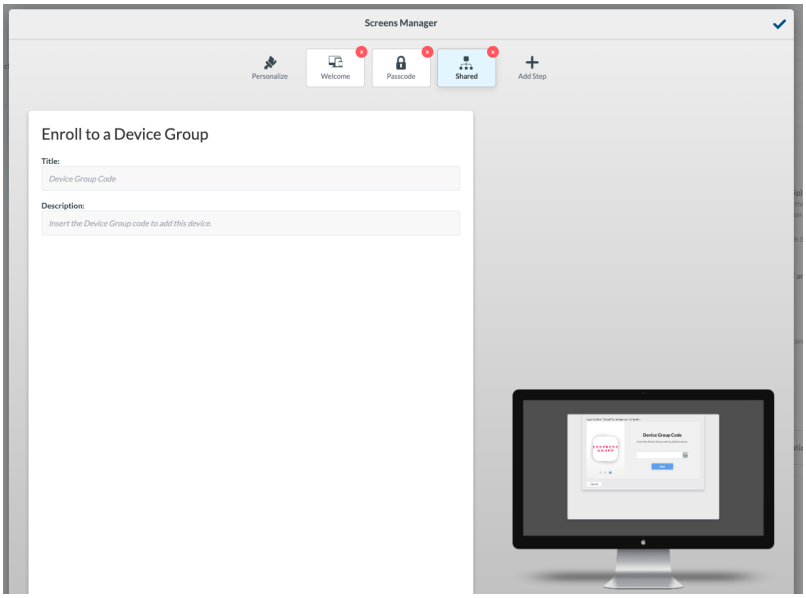
6.2 Ülevaade teisest sprindist – macOS seadme lisamine teise domeeni

II sprindi planeerimise koosolek toimus 25. novembril ning seal osalesid autor ning IT süsteemide administraator, koosoleku käigus kontrolliti, kas kõik I sprindi käigus tehtud tegevused on piisavad, et alustada II sprindiga ning määrati Scrum tahvlis algavaks sprindiks *backlogist* ülesanded, uuteks ülesanneteks olid: lisada macOS Setup Assistant aknasse uus vaheleht domeeni valimiseks, luua kaks seadmegruppi ekspress.ee ning ekspressgrupp.eu domeenidele, uute ettevõtte põhiste seadmegruppide loomine Mosyle haldusrakenduses, CIS poliitikate ülevaatamine ning vajadusel ajakohastamine ja muudetud deploy protsessi testimine. Sprindi eesmärgiks oli lisada macOS seade deploy jooksul teise domeeni nii, et kõik seni toimunud keskhalduse funktsionaalsused toimiksid ka uue domeeniga liidestatult.

II sprint algas 12.12.2022 ning lõppes 16.12.2022. Sprindi jooksul toimusid hommikuti kuni 15 minutilised koosolekud, kus arutati kuidas ülesannetega on läinud ning kas on töö tegemisel takistusi. Esimene sprint läks edukalt ning takistusi II sprindi ülesannetega alustamiseks polnud.

Sprindi alguses toimus IT osakonnas kasutusel oleva Jira piletihaldussüsteemi väljavahetamine – IT osakond võttis kasutusele Clickup keskkonna, seetõttu tuli sprindi alguses kasutusel olev Scrum *board* migreerida uude keskkonda. Clickupis asuva Scrum tahvliga on võimalik tutvuda Lisas 6 (lk 59).

Sprindi esimese ülesandena lisas autor Mosyle MDM teenuses macOS Setup Assistant aknasse uue vahelehe nimega "Enroll to a Device Group" ning lõi kaks koodi, millega lisada tööjaamad domeenidesse (Joonis 21). Enroll to a Device Group aknas on võimalik tänu uuele seadistusele trükkida sisse üks kahest koodist – sisestades esimene kood lisatakse arvuti ühte domeeni ning sisestades teine kood lisatakse arvuti teise domeeni.



Joonis 21. macOS Setup Assistant aknasse lisa lehe "Enroll to a Device Group" lisamine Mosyle teenuses

Teise ülesandena loodi Mosyle teenuses kaks uut seadmegruppi: ekspress.ee ning ekspressgrupp.eu – nii filtreeriti kahes erinevas domeenis olevad seadmed. Seejärel lõi autor 7 uut seadmegruppi esimesele tütarettevõttele, kelle seadmed lisatakse uude domeeni. Joonisel 22 (lk 38) on kirjeldatud loodud seadmegruppide nimetused ning nende tööpõhimõtted.

Seadmegrupi nimetus	Eesmärk
Apple Silicon Devices	Selekteerib gruppi seadmed, millel on Apple'i omaloodud protsessor.
CIS-LEVEL-2 Policy	Grupis olevatele seadmetele rakendatakse Mosyle teenuses aktiveeritud CIS Level 2 turvapoliitikad.
Detection & Removal Policy	Grupis olevatele seadmetele rakendatakse Mosyle Detection & Removal antiviiruse poliitikad.
FileVault disabled	Selekteerib gruppi seadmed, millel on FileVault deaktiveeritud.
Microsoft Office App	Gruppi lisatud seadmetele ilmub Self-Service rakenduses nähtavale Microsoft O365 installimise võimalus.
Privileges App	Gruppi lisatud seadmetele ilmub Self-Service rakenduses nähtavale Priviliges rakenduse installimise võimalus. (Rakendus võimaldab kasutajal piiratud aja jooksul olla arvutis administreerivate kasutajaõigustega)
Software Delay 0 days	Selekteerib gruppi seadmed, mis saavad uuendused kohe, kui need on Apple'i poolt välja lastud
Software Delay 7 days	Selekteerib gruppi seadmed, mis saavad uuendusi 7 päeva pärast nende väljaandmist Apple'i poolt.
Software Delay 14 days	Selekteerib gruppi seadmed, mis saavad uuendusi 14 päeva pärast nende väljaandmist Apple'i poolt.

Joonis 22. Mosyle teenuses loodud seadmegruppide põhimõtted

Peale seadmegruppide loomist vaatas autor koos IT süsteemide administraatoriga üle kasutusel Mosyle teenuses olevad aktiivsed CIS poliitikad ning nendes tehti osaliselt muudatusi. Lõpetuseks testis autor koos IT tehnikuga muudetud *deploy* protsessi. Võeti uus macOS seade ning alustati selle *deployd*, uues Enroll to a Device Group aknas sisestati autori loodud teine kood, millega lisati seade uude domeeni. *Deploy* protsess läks edukalt – arvutisse oli võimalik sisse logida teise domeeni kasutajaga, NoMAD rakendus toimis ning sünkroniseeris andmeid, läbi NoMAD Login rakenduse tehtud paroolivahetus oli edukas. II sprindi kokkuvõttev koosolek ning retrospektiiv toimusid 19.12.2022 – otsustati, et loodud lahendus toimib hästi kuid tulevikus macOS Setup Assistant aknasse võimaluse korral enam uusi avalehti ei lisata vaid kaalutakse muid süsteemseid variante, et vältida *deploy* alustamise protsessi pikaks venimist.

Teise sprindi jooksul tehtud ülesanded ning sprindi käigus täidetud nõuded on kirjeldatud joonisel 23 (lk 39).

Nr	Eesmärk ning inkrement	Tehtavad ülesanded	Testimine	Sprindi jooksul täidetud nõuded
Sprint II 12.12.2022- 16.12.2022	Lisada macOS seade deploy jooksul teise domeeni. **Inkrement** - teises domeenis asuv macOS seade.	1. macOS Setup Assistant aknasse lisa lehe lisamine; 2. ekspress.ee ja ekspressgrupp.eu gruppide loomine 3. Uute seadmegruppide loomine; 4. CIS poliitikate ülevaatamine. 5. Muudetud deploy protsessi testimine.	1. Integratsiooni-testimine; 2. Regressioon-testimine.	1. Tööjaamad peavad vastama CIS Level 2 turvastandardile 2. Sisselogimine macOS arvutitesse läbi mitme Windows domeeni; 3. Seadmete ettevalmistamisel peab olema võimalik valida mitme domeeni vahel; 4. Kasutajatel on keelatud rakenduste sätete omavoliline muutmine; 5. Arvutisse sisselogimine peab piirduma maksimaalselt kahe sisselogimise korraga. 6. Kasutaja peab saama arvutisse sisse logida Windows domeeni sisselogimise andmetega; 7. Seadmetes muudatuste rakendamine toimub kasutajale märkamatult ning ilma kasutaja sekkumiseta; 8. Võimalus üksikult lisada või eemaldada rakendatud turvapoliitikaid.

Joonis 23. II sprindi ülevaade

Sprindi tulemusel lisati macOS seade deploy jooksul teise domeeni ning vastavalt joonisel kirjeldatule täideti sprindi jooksul 8 nõuet.

6.3 Ülevaade kolmandast sprindist – macOS seadme tõrgeteta kasutamine ja üleandmine kasutajale

III sprindi planeerimise koosolek toimus 13. jaanuaril 2023 ning seal osalesid autor ning IT süsteemide administraator – sprindi eesmärgiks määrati keskhalduses oleva (teises domeenis asuva) seadme tõrgeta kasutamine ning kasutajale üle andmine. Selle eesmärgi saavutamiseks määrati tehtavateks ülesanneteks:

- Self-Service's rakenduste uuendamine, et kasutajatel oleks kõik vajalik tarkvarakataloogis olemas.
- *Custom commands* rakendamine - rakendada uue domeeniga seotud seadmetele seni keskhalduses kasutusel olnud erilised skriptid, näiteks TeamVieweri rakenduse installimine, seadmega ühendatud monitori seerianumbri logimine, arvuti prügikasti tühjendamine 30 päeva möödudes jne.
- Võrguketaste lisamine Maci *docki* vaatesse.
- Testimine ning lahenduse dokumenteerimine.

III sprint algas 16.01.2022 ning lõppes 20.01.2023. Sprindi käigus lahendati määratud ülesanded ning lõpuks anti kasutajale toimiv macOS seade. Autor dokumenteeris macOS seadme uuendatud *deploy* protsessi. III sprindi ülevaade on nähtaval joonisel 24 (lk 40).

Nr	Eesmärk ning inkrement	Tehtavad ülesanded	Testimine	Sprindi jooksul täidetud nõuded
Sprint III 16.01.2023- 20.01.2023	Keskhalduses oleva teises domeenis asuva seadme tõrgeteta kasutamine ning kasutajale üle andmine. **Inkrement** - kasutaja kasutab teises domeenis olevat macOS seadet.	1. Uuendada Self-Service's rakendused. 2. Custom commands rakendamine; 3. Testimine; 4. Võrguketaste lisamine Docki vaatesse; 5. Lahenduse dokumenteerimine.	1. Süsteemtestimine; 2. Kasutatavuse testid.	1. Peab tuginema E-ITS standardile nii palju kui võimalik; 2. Automaatne sisselogimine võrguressurssidele; 3. Teenus peab olema rakendatud kõikides macOS seadmetes; 4. Kõikides seadmetes peab olema ühtne kasutuskogemus; 5. Keskhaldusteenuse klienttarkvara ei tohi arvuti jõudlust kasutajale märgataval viisil mõjutada; 6. Uute Windows domeenide lisamise tööprotsess peab olema dokumenteeritud; 7. Ettevõtete halduspringsiibid peavad olema dokumenteeritud.

Joonis 24. III sprindi ülevaade

III sprindi kokkuvõttev koosolek ning retrospektiiv toimusid 23. jaanuaril – hinnati loodud protsessi ning lahendust ja määrati tööalane eesmärk esimese kontserni tütarettevõtte Apple'i seadmete keskhaldusesse liidestamiseks. Sprindi seatud eesmärk sai sooritatud – *deploytud* seadet oli võimalik tõrgeteta kasutada ning esimesed lõppkasutajad said uues domeenis olevad arvutid enda kasutusse.

Sprint sai edukalt lõpetatud. Sprintide jooksul lõi autor olemasolevasse keskhaldussüsteemi uue funktsionaalsuse, tänu millele on kasutajatel võimalik ennast macOS seadmetes erinevatest domeenidest autentida.

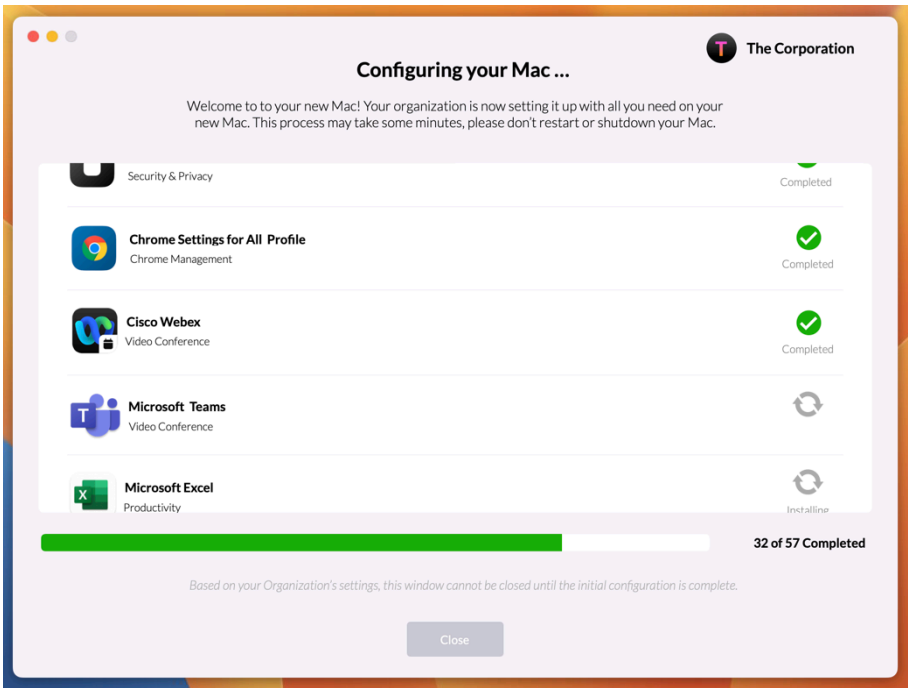
7 ETTEPANEKUD KESKHALDUSE EDASISEKS ARENDAMISEKS

Lõputöö sissejuhatuses kirjeldatud aastatega järjepidevalt kasvav küberintsidentide ja küberrünnakute arv Eestis rõhutab selgelt vajadust ettevõtetes nii aktiivselt kui ka proaktiivselt alustada IT teadlikkuse ning küberturvalisuse parendamisega. Värskelt jõustunud E-ITS infoturbestandardi järgi on ettevõtetes seadmete turvalisuse tagamise üheks parimaks praktikaks keskhaldustarkvara kasutamine – tegemist on sülearvutite turvalisuse tagamise kõrgeima meetmega. MDM tarkvara kasutamine on kõige tõhusam meetod Apple'i seadmete turvaliseks haldamiseks mis tahes ettevõttes. Autori hinnangul on võimalik kontsernis kasutatavat Apple'i seadmete keskhaldussüsteemi veelgi tehniliselt täiustada ning muuta, et süsteemi veelgi rohkem kaasajastada.

Autori esimeseks ettepanekuks on MDM rakenduses Mosyle Embark featuuri kasutusele võtmine. Featuuriga on võimalik automatiseerida peale seadmete ettevalmistamist standardtarkvara installimine tööjaamadesse (et seda ei peaks tegema ei IT tehnik ega ka mitte kasutaja) ning seeläbi parandada ka uue töötaja esimese tööpäeva kogemust. Hetkel on tegemist beetaversioonis oleva MDM rakenduse täiendusega, mida on võimalik juba testida. Mosyle Embark rakendus käivitatakse arvutis peale kasutaja esmast sisselogimist ning seejärel toimuvad järgmised toimingud:

1. Rakendus veendub, et arvutil on piisavalt akut, et lõpetada tarkvarade ning konfiguratsioonide installeerimine.
2. Kui seadmel on piisavalt toidet ilmub kasutajale aken, kus on visualiseeritud edusammudena rakenduste installeerimise ning seadistuse olek, kasutajat teavitatakse ning juhendatakse uue Maci seadistamise käigus.
3. Rakendus teavitab kasutajat, et ta hoiaks sülearvuti kaane avatuna.
4. Peale vajalike seadistuse installimist arvuti taaskäivitatakse FileVaulti käivitamiseks (Mitchell, 2022).

Järgmisel joonisel (Joonis 25, lk 42) on kujutatud Mosyle Embark rakenduse vaadet, mida kuvatakse kasutajale peale esmast arvutisse sisselogimist.



Joonis 25. Mosyle Embark rakenduse vaade (Mosyle Corporation, 2022)

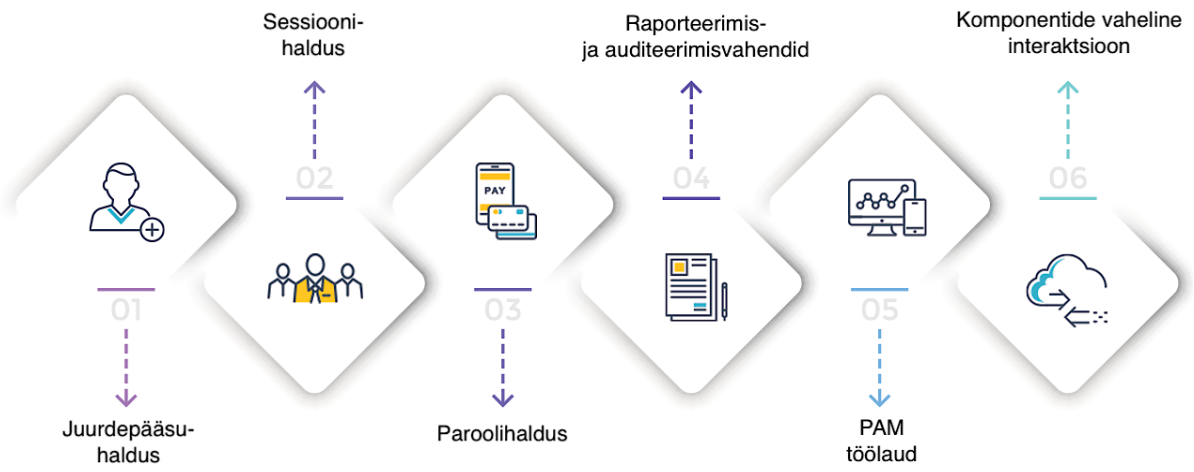
Teiseks ettepanekuks on hetkel erinevates failiserverites asuvate kaustade/võrguketaste migreerimine pilveteenusesse. Autori hinnangul võiks ettevõtetes kasutusel olevate dokumentide haldamiseks kasutada võrguketaste asemel näiteks Microsoft Sharepoint pilvepõhist platvormi. Sharepoint on hea alternatiiv võrguketastele, peamised põhjused, miks võiks eelistada Sharepointi on:

- Kasutajatel ei ole vaja olla sisevõrgus või ühendada ennast VPNiga sisevõrku selleks, et pääseda ligi dokumentidele.
- Ei ole vaja eraldi luua Mosyle Business rakenduses Mac'i *docki* konfiguratsioone.
- Mugav juurdepääsuõiguste kontroll – Sharepointis on võimalik mugavalt jagada juurdepääsuõiguseid erinevate kasutajate või gruppide vahel.
- Võimalus töövooge automatiseerida – näiteks kindlas kaustas olevad dokumendid suunatakse kindlale osakonnale või inimesele allkirjastamiseks.
- Tõhusam dokumentide haldus – Sharepoint võimaldab dokumente organiseerida mitmetel erinevatel viisidel, näiteks metaandmete järgi, märksõnade abil, kaustade kaupa jne.
- Parem kööstöö – meeskonnaliikmed saavad samaaegselt töötada ühe dokumendi kallal, kõiki tehtud muudatusi saab versiooniajaloos vaadata ning vajadusel vanem versioon dokumendist kiirelt ja lihtsalt taastada (*SharePoint – dokumendihaldus ja palju muud*, s.a.).

Kolmandaks ettepanekuks on juurutada kontsernis eriõigustega kontode ehk eeliskontode haldamine (*privileged access management,* PAM). Eriõigustega kontode haldusega on võimalik turvata süsteemides olevaid administreerivaid kontosid. Kasutades taolist lahendust on ettevõttes võimalik:

- Reguleerida ligipääsuõiguste jagamist.
- Jälgida ning auditeerida eriõigustega kontode tegevusi, tänu millele on võimalik teha järeldusi, kas on vaja näiteks õiguseid piirata või lisada juurde.
- Tagada eriõigustega juurdepääs vaid kindlatel kasutajatel, kindlatele rakendustele või kindlatele infosüsteemi osadele.
- Lisada kasutajakontodele kõrgemad ligipääsuõigused vastavalt tööülesannetele või ametikohale.
- Luua eelispääsuga kontod – tavakasutajakontod, mis on kõrgendatud õigustega.

Joonisel 26 on kirjeldatud eriõigustega kontode haldamise võtmekomponendid.



Joonis 26. Eriõigustega kontode haldamise süsteemi võtmekomponendid (Mohanakrishnan, 2021)

Võtmekomponentideks on: juurdepääsuhaldus, sessioonihaldus, paroolihaldus, raporterimis- ja auditeerimisvahendid, PAM töölaud ning komponentide vaheline interaktsioon. Seni kasutusel oleva meetodi, kus administreerivaid õiguseid jagatakse tööjaamades kasutades Privileges rakendust soovitab autor välja vahetada, sest sellisel moel antakse administreerivad õigused kasutajatele küll kindlaks ajavahemikuks, kuid kuidagi ei ole piiratud, mida kasutajad installeerivad või mida täpselt eriõigustega teevad – seda ei ole võimalik ka tagasiulatuvalt auditeerida.

Autori neljandaks ettepanekuks on liikuda autentimisega Azure Active Directory peale ning kaotada kohalikud olemasolevad domeenid. Mihhail Shumenkov defineerib Datafoxi blogipostituses Azure

Active Directory (Azure AD) kui Microsofti multi-tenant teenust, mis tagab pilveteenuste identiteedi- ja ligipääsuhalduse ärikriitilisel tasemel (Shumenkov, 2022). Azure AD võimaldab luua ja hallata kasutajakontosid – selliselt oleks Windows domeenis olevate kasutajakontode liidestamine Mosyle MDM rakendusega lihtsam ning tulevikus tekiks võimalus liikuda ka näiteks Windowsi seadmetega praegu kasutusel olevast Microsoft System Center Configuration rakendusest pilvepõhise Microsoft Intune peale.

Viiendaks ettepanekuks on arvuti *deploy* protsessi edasine automatiseerimine ning seeläbi IT süsteemide administraatori eemaldamine töövoost. Autori hinnangul võiks seadmete *deploy* protsessi muuta selliselt, et IT süsteemide administraator ei peaks protsessis üldse vahel olema – see kiirendaks seadmete ettevalmistamise protsessi veelgi. Hetkel kasutusel olevad konfiguratsiooniprofiilid on tarvis *deploy* protsessi ajal kindlas järjekorras installeerida – sel põhjusel on ka IT süsteemide administraatori vahel olemine oluline, tema määrab peale esmaste profiilide installimise järgmised profiilid. Kui võtta kasutusele autori neljandas ettepanekus välja toodud Azure AD ei oleks vaja enam sellisel kujul kasutada praeguseid konfiguratsiooniprofiile ning oleks võimalik muuta lahendust nii, et *deploy* protsessis ei pea peale IT tehniku kedagi olema.

Viimaseks ettepanekuks on ettevõtete põhise brändingu kasutamine keskhaldusesse lisatud seadmetes. Mosyle teenus võimaldab ettevõttepõhiselt konfigureerida ning hallata arvutites olevaid töölaua ning lukustuskuva taustapilte. Autor soovitab rakendada MDM teenust kasutades ettevõtete põhist brändingut just taustapiltide näol. Ettevõttepõhised taustapildid aitavad suurendada brändi nähtavust – näiteks eeldusel, et seadme taustapildiks on määratud ettevõtte logo koos peamise sõnumiga ja töötaja kasutab tööarvutit avalikus kohas kohtumisel või muul viisil töö tegemiseks panevad ümbruses olevad inimesed üldjuhul pilte tähele ja seeläbi suurendatakse ettevõtte tuvastamise tõenäosust.

KOKKUVÕTE

Lõputöö teemaks oli Apple tööjaamade haldus mitme domeenivõrguga suurettevõttes. 2020. aastal juurutati Ekspress Grupis Apple tööjaamade keskhaldustarkvara Mosyle Business, kuid seni puudus võimalus keskhaldussüsteemis seadmeid lisada mitmesse domeeni – seetõttu oli võimalus keskhaldust reaalselt kasutada vaid ühel tütarettevõttel, Delfi Meedial (kontsernis on kokku 14 tütarettevõtet).

Lõputöö käigus loodi ning implementeeriti olemasolevasse keskhaldussüsteemi uus funktsionaalsus, tänu millele on võimalik erinevate Windowsi domeenide kasutajatel ennast halduses olevates Apple seadmetes autentida – ehk enam pole takistusi haldustarkvara juurutamiseks kõigis tütarettevõtetes.

Juurutusprojekti esimeses osas kirjeldas autor Apple tööjaamade senist haldust kontserni ettevõtetes *(as-is)*, analüüsis lähtuvalt E-ITSi etalonturbe kataloogist Apple seadmete käsitsi seadistamise protsessi ja arvuti edasist kasutust (ilma keskhalduseta ettevõtte näitel) ning kirjeldas projekti ajakava. Seejärel andis autor ülevaate Apple tööjaamade keskhalduse teoreetilistest lähtekohtadest ning kirjeldas seadmete keskhaldussüsteemi liidestamise protsessi.

Lisatava funktsionaalsuse loomise esimese etapina alustas lõputöö autor koostöös IT süsteemide administraatori ning IT kasutajatoe juhiga vajalike nõuete kaardistamise ning prioritiseerimisega. Nõuete kaardistamiseks kasutas autor laialt levinud FURPS metoodikat ning prioritiseerimiseks MoSCoW meetodit, tulemused kirjeldati tabelitena.

Funktsionaalsuse loomiseks valis autor agiilse Scrum raamistiku. Autori hinnangul raamistiku peamisteks eelisteks on – paindlikkus, meeskonnatööle orienteeritus ning jooksvalt projekti muudatuste sisseviimise lihtsus. Funktsionaalsuse arendus toimus kolme sprindi jooksul.

Projekti arenduskäiku ning testimist on lõputöö autor kirjeldanud töö viiendas peatükis, tuues välja sprindi jooksul tehtud ülesanded, testimine ja sprindi jooksul täidetud nõuded. Esimese sprindi eesmärgiks oli luua uue domeeni jaoks konfiguratsiooniprofiilid, teise sprindi eesmärgiks lisada macOS seade deploy jooksul teise domeeni ning viimase sprindi eesmärgiks keskhalduses oleva seadme tõrgeteta kasutamine ning kasutajale üle andmine.

Eelviimases ehk kuuendas peatükis toob autor välja omapoolsed kuus ettepanekut kontsernis keskhalduse edasiseks arendamiseks, nendeks on:

- Võtta MDM rakenduses kasutusele Mosyle Embark featuur.

- Asendada hetkel kasutuses olevad võrgukettad Sharepointi pilveteenusega.
- Juurutada kontsernis eriõigustega kontode ehk eeliskontode haldamine (*privileged access management*, PAM).
- Viia kasutajakontode autentimine Azure AD peale.
- Automatiseerida Mac arvutite *deploy* protsessi selliselt, et IT süsteemide administraator ei peaks töövoos enam olema.
- Kasutada ettevõtte põhist brändingut läbi MDM teenuse.

Lõputöö tulemusel on loodud ning juurutatud lahendus keskhaldussüsteemist mitmest domeenist autentimiseks – tänu millele on võimalik keskhaldusrakendus võtta kasutusele kontserniüleselt. Loodud lahendusega tõhustatakse tööjaamade turvameetmeid ning seeläbi parendatakse ettevõtetes tunduvalt küberturvalisust. Keskhaldusega on võimalik saada mugavalt ülevaade ettevõttes kasutusel olevatest varadest, monitoorida kasutajate kasutuses olevaid seadmeid, kontrollida tööjaamade olekut, uuendada tööjaamades tarkvara ning kõige tähtsam – seadmeid on võimalik keskselt hallata ning rakendada turvapoliitikaid.

Autori hinnangul said kõik töö alguses püstitatud eesmärgid sooritatud.

SUMMARY

The title of this thesis is ***Management of Apple workstations within a large enterprise with multiple domain networks.***

This thesis consists of six chapters with a total of 61 pages. The chapters of this thesis are: An overview of Ekspress Grupp's media group and an analysis of Apple workstation management in their companies (as-is); Theoretical Basis for Centralized Apple Workstation Management (as-is); Mapping and Prioritizing requirements; Theoretical and methodological framework for the development, testing and implementation of additional functionality; Creating, Testing and implementing new functionality in the media group and the last chapter is proposals for further development of the central management.

The thesis consists of 26 figures, 3 tables and is based on 45 references, mostly digital articles or books in Estonian and English and diploma works.

Based on the results of Cyber Security Yearly Assessments made in 2021, 2022 and 2023 by Estonian Information System Authority (RIA), the increase in the number of cyber incidents in Estonia over the past few years demonstrates that security vulnerabilities, outdated software and device configuration errors can lead to cyber attacks that can impact our daily lives. Management of Apple workstations (MDM) is highly advisable by Estonian Information Security Standard (E-ITS) for companies of various sizes. MDM software allows organizations to centrally manage their workstations, enforce security policies, disable specific features or applications for end users, check the status of devices and additionally, it simplifies the process of assisting end users.

The aim of the thesis is to create and implement the functionality of a centralized management system (MDM) to allow users to authenticate from various Windows domains thereby making it possible to implement centralized Apple Workstation Management in Ekspress Grupp's companies.

The following tasks have been created to achieve the goal of the thesis:

- To describe the existing system *(as-is).*
- To analyze the compliance of the workflow used in companies with the E-ITS information security standard and determine the project schedule.
- To describe the requirements for the additional functionality to be added.
- To prioritize the described requirements.

- To select a suitable development methodology.
- To create and implement functionality for authenticating from various Windows domains.
- To make suggestions for further improvement of the central management software.

Author analyzed current management of Apple devices in Ekspress Grupp's companies using Estonian Information Security Standard (E-ITS). The requirements for the additional functionality were defined by the author using the FURPS methodology and prioritized using the MoSCow method. Functionality was developed using the agile framework Scrum. For testing black box methodology and Integration testing, System testing, Regression testing and Usability testing methodologies were used.

After implementing the functionality author proposed the following suggestions for further improvement of the central management software:

- Author suggests enabling the Mosyle Embark feature in the MDM application.
- Replace the currently used network drives with SharePoint cloud service.
- Implement privileged access management (PAM) to improve security, compliance, accountability, and operational efficiency in companies.
- Migrate user account authentication to Azure AD.
- Automate the Mac computer deployment process in such a way that the IT systems administrator no longer needs to be involved in the workflow.
- Utilize enterprise branding through MDM service.

In the author's opinion, all the goals of this thesis have been achieved: current management of Apple devices was analyzed, a new functionality to allow users to authenticate from various Windows domain through MDM was developed and implemented. In the end, the author provided suggestions for improving central management of Apple devices.

VIIDATUD ALLIKAD

Adams, K. MacG. (2015). „*Nonfunctional Requirements in Systems Analysis and Design*" (Kd 28). Springer International Publishing. https://doi.org/10.1007/978-3-319-18344-2

AKIT - „*Andmekaitse ja infoturbe leksikon*." (2022, mai 11). https://akit.cyber.ee/term/5722

Akiwatkar, R. (2022, november 10). State of Agile Adoption 2023: „How is Software Development changing?" *Simform - Product Engineering Company*. https://www.simform.com/blog/state-of-agile-adoption/

Apple Inc. (2017). „*Volume Purchase Program Guide*." 8.

AS Ekspress Grupp. (2022). „*AS Ekspress Grupp Konsolideeritud majandusaasta aruanne 2021*." AS Ekspress Grupp. https://2021-annual-report.egrupp.ee/assets/pdf/EkspressGruppkonsolideeritud2021_EST2.pdf

„*Atlassiani tooted*." (s.a.). Trinidad Wiseman | Atlassian. Salvestatud 30. märts 2023, https://atlassian.twn.ee/atlassiani-tooted/

Bottorff, C., & Crail, C. (s.a.). „*What Is A Scrum Board? – Forbes Advisor*." Salvestatud 5. aprill 2023, https://www.forbes.com/advisor/business/what-is-a-scrum-board/

Center fot Internet Security, Inc. (2019, aprill 1). „*CIS meetmed*" (AS BCS Koolitus, Tõlk). https://www.ria.ee/sites/default/files/content-editors/kuberturve/cis20_meedet_eesti_keeles.pdf

Dreyer, A., & Karneboge, A. (2016). „*Managing Apple Devices: Deploying and Maintaining iOS 9 and OS X El Capitan Devices*." Peachpit Press.

Edge, C., & Trouton, R. (2019). „*Apple Device Management: A Unified Theory of Managing Macs, iPads, iPhones, and AppleTVs*" (1st ed. edition). Apress.

„*Eesti Infoturbestandard*." (s.a.). Salvestatud 14. märts 2023, https://eits.ria.ee/

„*E-ITS Tutvustus*." (s.a.). Salvestatud 18. aprill 2023, https://eits.ria.ee/et/avalehe-menueue/tutvustus/

Ekspress Grupp AS. (2022). „*Meie tegevusvaldkonnad – Ekspress Grupp*." https://www.egrupp.ee/grupist/meie-tegevusvaldkonnad/

Evans, J. (2021, aprill 5). „*Mosyle unveils Apple MDM tools for the enterprise*." Computerworld. https://www.computerworld.com/article/3614082/mosyle-unveils-apple-mdm-tools-for-the-enterprise.html

Gloger, B., Pfarl, W., Mittermayr, R., & Opelt, A. (2013). „*Agile Contracts: Creating and Managing Successful Projects with Scrum*." John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/nlibee-ebooks/detail.action?docID=1191572

Güzelsevdi, C. (2021, september 29). „What is MoSCoW Analysis and MoSCoW Method?" *Projectcubicle*. https://www.projectcubicle.com/what-is-moscow-analysis-and-moscow-method/

„*Infoturbe soovituste juhend*." (2009). https://www.ria.ee/sites/default/files/content-editors/ISKE/infoturbe_soovituste_juhend_v1.pdf

Jamwal, D. D. (2010). „*Analysis of Software Quality Models for Organizations*" (Nr 2). *1*(2), Article 2.

Kehtna Kutsehariduskeskus. (2018, detsember 6). *MoSCoW – „Teadmusbaas*." http://wiki.kehtna.edu.ee/MoSCoW

Kõrgmaa, R. (2021). „*Pipedrive*." Valge Klaar. https://valgeklaar.ee/apple-business-manager/pipedrive/

„*Küberturvalisuse aastaraamat 2022*." (2022). https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_kyberturvalisuse_aastaraamat_2022_est_veeb.pdf

„*Küberturvalisuse aastaraamat 2023*." (2023). https://www.ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid

Leviatan, A. (2022, detsember 6). „*Getting started with iMazing Profile Editor*." https://imazing.com/guides/getting-started-with-imazing-profile-editor

„*Manifesto for Agile Software Development*." (2001). https://agilemanifesto.org/

MarketsandMarkets. (2022). „*Mobile Device Management Market Size, Share and Global Market Forecast to 2026 | COVID-19 Impact Analysis | MarketsandMarkets*." https://www.marketsandmarkets.com/Market-Reports/mobile-device-management-market-105562389.html

Mitchell, K. (2022, oktoober 4). „*Mosyle Embark Creates Seamless Day One Experiences for Employees Using Mac Devices at Work*." https://www.businesswire.com/news/home/20221004005252/en/Mosyle-Embark-Creates-Seamless-Day-One-Experiences-for-Employees-Using-Mac-Devices-at-Work

Mohanakrishnan, R. (2021, august 30). „What Is Privileged Access Management (PAM)? Definition, Components, and Best Practices." *Spiceworks*. https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-privileged-access-management/

„*MoSCoW Prioritization*." (s.a.). Salvestatud 17. aprill 2023, https://www.productplan.com/glossary/moscow-prioritization/

Mosyle Corporation. (2022). „*Mosyle Business*." https://business.mosyle.com/

Oixio AS. (2021, september 21). „Kuidas kaitsta nutiseadmes olevaid äriandmeid?" *Ärigeenius*. https://ari.geenius.ee/blogi/oixio-blogi/kuidas-kaitsta-nutiseadmes-olevaid-ariandmeid/

Orchard & Grove Inc. (2022). „*About NoMAD | NoMAD*.” https://nomad.menu/about-nomad/

PeopleCert International Ltd. (2022, august 12). *PeopleCert*. „The world’s most widely used IT Service Management framework.” https://www.peoplecert.org/ITIL-4

Petuhhov, I. (2011). „*Testimise tüübid*.” Infosüsteemi hankimine, arendus ja teostamine. https://eopearhiiv.edu.ee/e-kursused/eucip/arendus/143_testimise_tbid.html

Petuhhov (TLÜ), I. (2023). „*Agiilne tarkvaraarendus*.” http://www.cs.tlu.ee/~inga/TTP/Agiilsed_meetodid_2019.pdf

Pihlak, P. (2022, detsember 8). „*Valitsus kehtestas Eesti infoturbestandardi, mis aitab juhtida riske ja kaitsta infosüsteeme | Majandus- ja Kommunikatsiooniministeerium*.” https://mkm.ee/uudised/valitsus-kehtestas-eesti-infoturbestandardi-mis-aitab-juhtida-riske-ja-kaitsta-infosusteeme

„*SharePoint – dokumendihaldus ja palju muud*.” (s.a.). BRS Networks Baltic AS. Salvestatud 4. aprill 2023, https://www.brsnetworks.ee/blogi/motteid-it-teemadel/sharepoint

Shumenkov, M. (2022, aprill 11). „*Azure Active Directory turvameetmed tõstavad oluliselt digiidentiteedi turvalisust*.” https://www.datafox.ee/et/blogi/532-azure-active-directory-turvameetmed-tostavad-oluliselt-digiidentiteedi-turvalisust

SYS.3.2.2: „*Mobiilseadmete haldus (MDM)*.” (s.a.). Salvestatud 18. aprill 2023, https://eits.ria.ee/et/versioon/2022/etalonturbe-kataloog/sys-itsuesteemid/sys3-mobiilseadmed/sys32-nutitelefon-ja-tahvelarvuti/sys322-mobiilseadmete-haldus-mdm/

Tepandi, J. (2022, detsember 3). „*Tarkvara protsessid ja kvaliteet*.” http://tepandi.ee/tks-loeng.pdf

Trudel, J. (2016). „5 „best practices“ for mobile device management.” *New Hampshire Business Review*, *38*(12), Article 12.

Valge Klaar. (2018). „*Apple Business Manager*.” Valge Klaar. https://valgeklaar.ee/apple-business-manager/

Veldre, A. (2016, juuni 9). „*Kuidas hoiduda olukorrast, kus pahavara arvutis asuvad failid pantvangi võtab*.” Forte. https://forte.delfi.ee/a/74465191

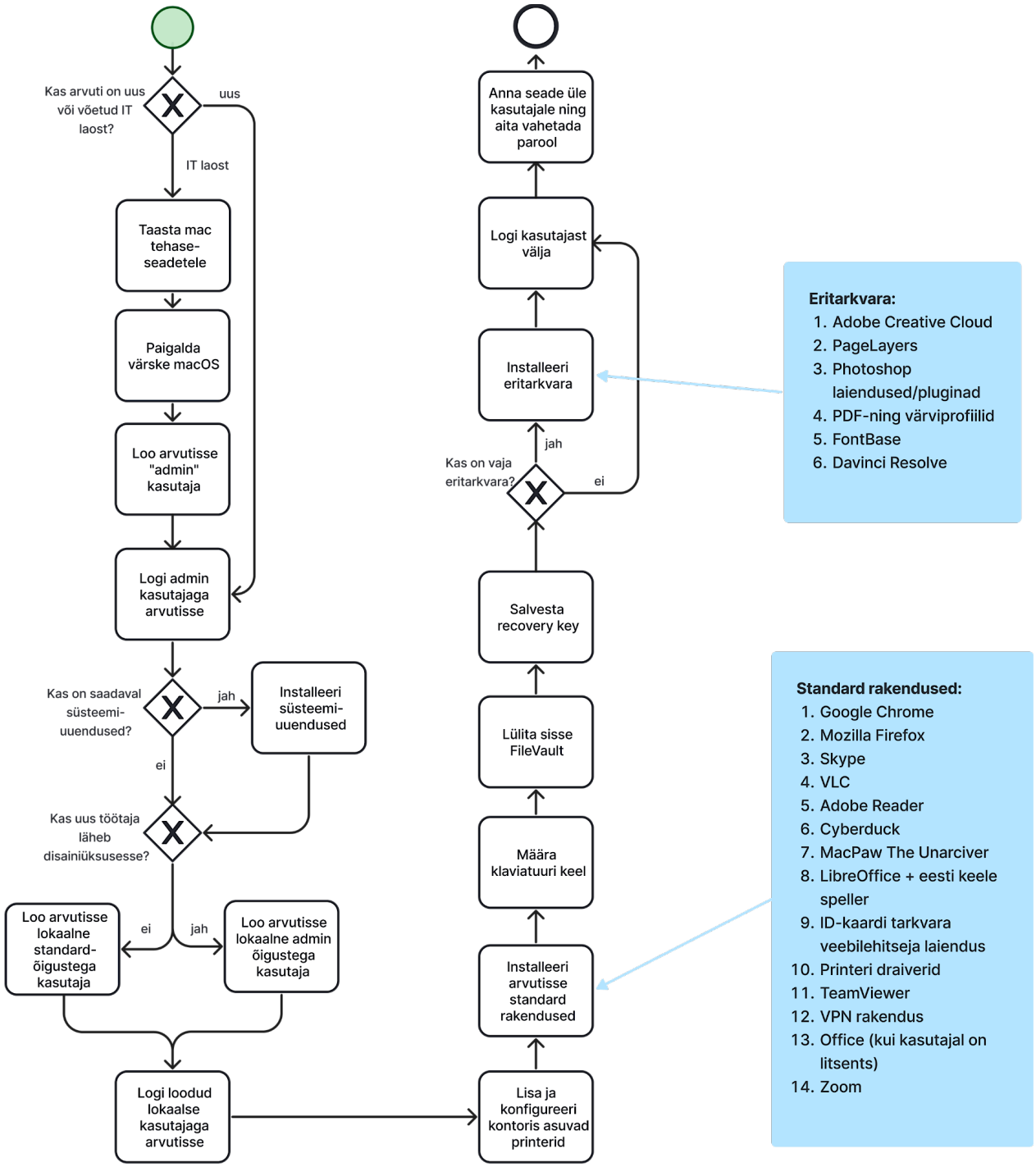
Viscardi, S. (2013). „*The Professional ScrumMaster’s Handbook*.” Packt Publishing, Limited. http://ebookcentral.proquest.com/lib/nlibee-ebooks/detail.action?docID=1192653

Vorteil, V., & Laanpere, J. (2023). „*Tarkvara testimise alused*.” https://web.htk.tlu.ee/digitaru/testimine/chapter/tarkvara-testimise-alused/

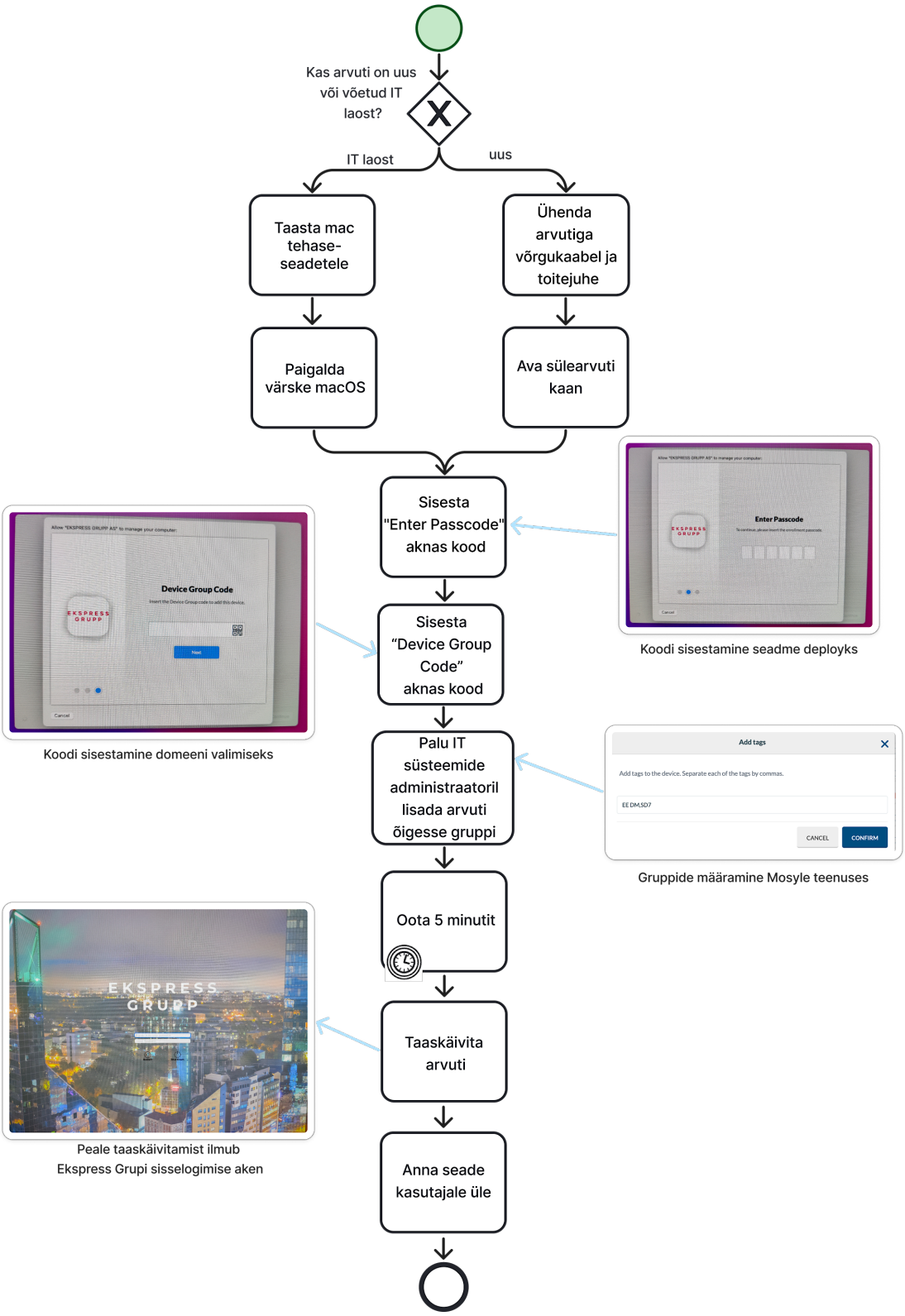
„*What is Privileged Access Management (PAM) | Microsoft Security*.” (s.a.). Salvestatud 4. aprill 2023, https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam

LISAD

Lisa 1. Arvuti käsitsi seadistamise tööprotsess (*as-is*)



Lisa 2. Arvuti keskhaldusesse lisamise tööprotsess (*to-be*)



Lisa 3. Projekti ajakava

Nr	Tegevus	Kaasatud inimesed	Tegevuse algus	Tegevuse lõpp
1	Esimene koosolek	Projektijuht, IT süsteemide administraator	16.02.2022	16.02.2022
2	Olemasoleva süsteemi kirjeldamine (*as-is*)	Projektijuht	17.02.2022	24.02.2022
3	Apple'i seadmete keskhaldussüsteemi liidestamise protsessi kirjeldamine	Projektijuht, IT süsteemide administraator	28.02.2022	02.02.2022
4	Kasutusel oleva tööprotsessi (*as-is*) (domeeniväliste Mac seadmete ettevalmistamine ja edasine haldamine) analüüsimine ja *to-be* tööprotsessi kirjeldamine	Projektijuht	03.02.2022	07.02.2022
5	Lisatava funktsionaalsuse nõuete kaardistamine	Projektijuht, IT kasutajatoe juht, IT süsteemide administraator	09.03.2022	09.03.2022
6	FURPS tabeli loomine	Projektijuht	10.03.2022	10.03.2022
7	Lisatava funktsionaalsuse nõuete prioritiseerimine	Projektijuht, IT süsteemide administraator	23.03.2022	23.03.2022
8	MoSCoW tabeli loomine	Projektijuht	24.03.2022	24.03.2022
9	Arendusmetoodika kokkuleppimine ja *backlogi* koostamine	Projektijuht, IT kasutajatoe juht, IT süsteemide administraator	19.10.2022	19.10.2022
10	I sprindi planeerimine ja sprindi backlogi koostamine	Projektijuht, IT süsteemide administraator, IT kasutajatoe juht	20.10.2022	20.10.2022
11	I sprint	Projektijuht, IT süsteemide administraator	14.11.2022	18.11.2022

Nr	Tegevus	Kaasatud inimesed	Tegevuse algus	Tegevuse lõpp
12	I sprindi järgne koosolek	Projektijuht, IT süsteemide administraator	22.11.2022	22.11.2022
13	I sprindi retrospektiiv	Projektijuht, IT süsteemide administraator	22.11.2022	22.11.2022
14	II sprindi planeerimine	Projektijuht, IT süsteemide administraator	25.11.2022	25.11.2022
15	II sprint	Projektijuht, IT süsteemide administraator	12.12.2022	16.12.2022
16	II sprindi järgne koosolek	Projektijuht, IT süsteemide administraator	19.12.2022	19.12.2022
17	II sprindi retrospektiiv	Projektijuht, IT süsteemide administraator	19.12.2022	19.12.2022
18	III sprindi planeerimine	Projektijuht, IT süsteemide administraator	13.01.2023	13.01.2023
19	III sprint	Projektijuht, IT süsteemide administraator	16.01.2023	20.01.2023
20	III sprindi järgne koosolek	Projektijuht, IT süsteemide administraator	23.01.2023	23.01.2023
21	III sprindi retrospektiiv	Projektijuht, IT süsteemide administraator	23.01.2023	23.01.2023
22	Esimeste arvutite *deploy* uude domeeni	Projektijuht, IT tehnik	30.01.2023	30.01.2023

Lisa 4. Lisatava funktsionaalsuse nõuete FURPS tabel

Funktsionaalsus	• Peab tuginema E-ITS standardile nii palju kui võimalik. • Sisselogimine macOS arvutitesse läbi mitme Windows domeeni. • MacOS konto tüüp peab olema lokaalne. • Automaatne sisselogimine võrguressurssidele. • Windows domeeni parooli muutmine peab olema võimalik läbi macOS tööjaama. • Windows domeeni ja macOS tööjaama paroolide sünkroniseerimine. • Tööjaamad peavad vastama CIS Level 2 turvastandardile. • Seadmete ettevalmistamisel peab olema võimalik valida mitme domeeni vahel. • Kasutajatel on keelatud rakenduste sätete omavoliline muutmine. • Võimalus mugavalt vajadusel vahetada domeeni, kus arvuti hetkel on. • Võimalus üksikult lisada või eemaldada rakendatud turvapoliitikaid.
Kasutatavus	• Teenus peab olema rakendatud kõikides macOS seadmetes. • Arvutisse sisselogimine peab piirduma maksimaalselt kahe sisselogimise korraga. • Kõikides seadmetes peab olema ühtne kasutuskogemus. • Kasutaja peab saama arvutisse sisse logida Windows domeeni sisselogimise andmetega. • Interneti puudumine ei tohi mõjutada arvutisse sisselogimist. • Seadmetes muudatuste rakendamine toimub kasutajale märkamatult ning ilma kasutaja sekkumiseta. • Kasutajal võimalus vaadata arvutist, mitme päeva pärast tema Windowsi domeeni parool aegub.
Käideldavus	• Haldusteenus peab olema majutatud välise teenusepakkuja pilvesüsteemis. • Haldusteenusesse ligipääsude loomisel lähtutakse minimaalõiguste printsiibist (POLP). • Seadmete haldusteenus ei tohi olla kättesaamatu rohkem kui 1 päeva kuus. • Seadmete haldusteenuse konfiguratsioon peaks olema varundatud teenusepakkuja juures.
Jõudlus	• Keskhaldusteenuse klienttarkvara ei tohi arvuti jõudlust kasutajale märgataval viisil mõjutada. • Masinate kogus süsteemis ei tohi mõjutada süsteemi enda võimekust. • Seadmehalduses tehtud muudatused peaksid jõudma seadmetesse 1 minuti jooksul.
Toetus	• Uute Windows domeenide lisamise tööprotsess peab olema dokumenteeritud. • Ettevõtete haldusprintsiibid peavad olema dokumenteeritud. • Teenusepakkuja tugi peaks olema kättesaadav vähemalt 24h jooksul.

Lisa 5. Lisatava funktsionaalsuse nõuete MoSCoW tabel.

Nr	Nõue	Prioriteet			
		M	**S**	**C**	**W**
1	Peab tuginema E-ITS standardile nii palju kui võimalik	X			
2	Sisselogimine macOS arvutitesse läbi mitme Windows domeeni.	X			
3	MacOS konto tüüp peab olema lokaalne.	X			
4	Automaatne sisselogimine võrguressurssidele.	X			
5	Windows domeeni parooli muutmine peab olema võimalik läbi macOS tööjaama.	X			
6	Windows domeeni ja macOS tööjaama paroolide sünkroniseerimine.	X			
7	Tööjaamad peavad vastama CIS Level 2 turvastandardile.	X			
8	Seadmete ettevalmistamisel peab olema võimalik valida mitme domeeni vahel.	X			
9	Kasutajatel on keelatud rakenduste sätete omavoliline muutmine.	X			
10	Teenus peab olema rakendatud kõikides macOS seadmetes.	X			
11	Arvutisse sisselogimine peab piirduma maksimaalselt kahe sisselogimise korraga.	X			
12	Kõikides seadmetes peab olema ühtne kasutuskogemus.	X			
13	Kasutaja peab saama arvutisse sisse logida Windows domeeni sisselogimise andmetega.	X			
14	Interneti puudumine ei tohi mõjutada arvutisse sisselogimist.	X			
15	Haldusteenus peab olema majutatud välise teenusepakkuja pilvesüsteemis.	X			
16	Haldusteenusesse ligipääsude loomisel lähtutakse minimaalõiguste printsiibist (POLP).	X			

Nr	Nõue	Prioriteet			
		M	**S**	**C**	**W**
17	Keskhaldusteenuse klienttarkvara ei tohi arvuti jõudlust kasutajale märgataval viisil mõjutada.	X			
18	Masinate kogus süsteemis ei tohi mõjutada süsteemi enda võimekust.	X			
19	Uute Windows domeenide lisamise tööprotsess peab olema dokumenteeritud.	X			
20	Ettevõtete halduspringsiibid peavad olema dokumenteeritud.	X			
21	Seadmetes muudatuste rakendamine toimub kasutajale märkamatult ning ilma kasutaja sekkumiseta.		X		
22	Seadmete haldusteenus ei tohi olla kättesaamatu rohkem kui 1 päeva kuus.		X		
23	Seadmete haldusteenuse konfiguratsioon peaks olema varundatud teenusepakkuja juures.		X		
24	Seadmehalduses tehtud muudatused peaksid jõudma seadmetesse 1 minuti jooksul.		X		
25	Teenusepakkuja tugi peaks olema kättesaadav vähemalt 24h jooksul.		X		
26	Võimalus üksikult lisada või eemaldada rakendatud turvapoliitikaid.			X	
27	Kasutajal võimalus vaadata arvutist, mitme päeva pärast tema Windowsi domeeni parool aegub.			X	
28	Võimalus mugavalt vajadusel vahetada domeeni, kus arvuti hetkel on.				X

Lisa 6. Projekti Scrum tahvel