TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Rait Rand 175042IDAR

Kasutajakonto elutsüklihalduse automatiseerimine Bolt Technology OÜ näitel

Diplomitöö

Juhendaja: Siim Vene
M.Sc.

Kaasjuhendaja: Martin Paroll
B.Sc.

Tallinn 2021

Autorideklaratsioon

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

Autor: Rait Rand

02.04.2021

Annotatsioon

Käesoleva diplomitöö eesmärgiks on Bolt Technology OÜ näitel esmalt kirjeldada ja modelleerida ning seejärel automatiseerida kasutajakontode elutsükli esimese etapi ehk töötaja liitumisega seonduvad manuaalselt tehtavad ülesanded. Töö teoreetilises osas antakse ülevaade IT-turvalisuse valdkonnast ning tööriistadest, mis vastavat automatiseerimist võimaldavad.

Töös vaadeldavaks probleemiks on kasutusel oleva värbamisprotsessi rohke manuaalse töö maht, aeglane info liikumine ning madal efektiivsus. Suurte värbamisvolüümide ning arvukate rakenduste haldamise tõttu on IT- ning personalimeeskonna töökoormus erakordselt kõrge. Sellest tulenevalt pole vastavate meeskondade laiendamine jätkusuutlik lahendus.

Töö käigus visualiseeritakse nii olemasolev kui ka uus värbamisprotsess ning kirjeldatakse vana protsessi kitsaskohti, mida uus protsess lahendab. Lisaks sätestatakse nõuded uuele protsessile ning viimase sammuna kirjeldatakse uue protsessi raames ühe rakenduse Oktaga liidestamiseks tehtavat tööd.

Töö tulemusena sai rakendatud värbamisprotsessi osa, mis vastutab kasutajakontode loomise, litsentseerimise ning ligipääsuõiguste andmise eest. Samuti automatiseeriti identiteetide loomine tsentraliseeritud kasutajakataloogi, personalitarkvarasüsteemi ning identiteeditеenuse omavahelise integreerimise kaudu.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 49 leheküljel, 7 peatükki, 26 joonist, 0 tabelit.

Abstract

Automating the Identity Lifecycle Flow in Bolt Technology OÜ

The aim of this diploma thesis is to first describe and model, then automate the manually performed tasks related to the first step of the user lifecycle. The theoretical part of the thesis provides an overview of the IT security field of identity and access management and the tools that it provides for enabling identity lifecycle automations.

The current onboarding process requires a large amount of manual work, is slow and inefficient. Due to the large onboarding volumes and managing numerous applications the workload of the IT and the HR teams is extremely high. Expanding the respective teams is not a viable long-term solution.

The work visualizes both the existing and the newly adopted onboarding processes and describes the bottlenecks of the old process, which the new process resolves. In addition to describing the two processes, the requirements for the new process are defined and finally the author describes the process of setting up an application with Okta.

As a result of this thesis a part of the user lifecycle flow which is responsible for creating user accounts, licencing and granting accesses was implemented. The identity lifecycle flow was also automated by implementing an HR as a source approach with our identity as a service provider, resulting in a centrally managed user directory.

The thesis is in Estonian and contains 49 pages of text, 7 chapters, 26 figures, 0 tables.

Lühendite ja mõistete sõnastik

AD	*Active Directory, Microsofti välja töötatud kataloogiteenus*
API	*Application Programmable Interface, programmiliides*
CRM	*Customer relationship management, kliendisuhete juhtimise tarkvara*
CSV	*Comma-separated values, komaeraldusega väärtused*
ERP	*Enterprise esource planning, Ettevõtte ressursside planeerimise tarkvara*
HRIS	*Human resource information system, personalijuhtimise infosüsteem*
IAM	*Identity and Access Management, Identiteet ja juurdepääsu haldamine*
IDaaS	*Identity as a Service, identiteet kui teenus*
MFA	*Multi-factor authentication, mitmeteguriline autentimine*
SCIM	*System for Cross-domain Identity Management, Süsteem domeenidevahelise identiteedi haldamiseks*
SSO	*Single-Sign On, ühekordne sisselogimine*

Sisukord

Jooniste loetelu

1 Sissejuhatus

Praktiliselt igas ettevõttes saab rääkida töötajate voolavusest, nendega seotud kasutajakontodest ning nende elutsüklihaldusest. Kõigi kaasatud osapoolte huvides on, et elutsükli haldusega seotud protsessid oleksid võimalikult efektiivsed, veakindlad ning info liikumine toimuks sujuvalt.

Tihtipeale jõuab ettevõtte kasvades kätte hetk, kus muutub aktuaalseks töötajate kasutajakontode elutsüklihaldusega seonduvate protsesside automatiseerimine. Töötajaskonna suurenedes ning hallatavate kontode ja rakenduste arvu kasvamisel muutub ligipääsuõiguste haldamine niivõrd komplekseks, et seda on võimalik hallata vaid väga suure meeskonnaga. Töös käsitletava ettevõtte kiire kasvuga kaasas käimiseks tekkis vajadus automatiseerida kasutajakontode elutsüklihalduse protsess kuid mahuliste piirangute tõttu võeti käesoleva töö skoobiks konkreetselt kasutaja värbamisprotsessiga seonduvad tegevused.

Manuaalsed protsessid kujutavad endast ebaefektiivset ressursikulu, võivad olla aeglased ning võrdlemisi veaohtlikud. Kasutajakonto elutsüklihaldusega seonduvate protsesside automatiseerimine aitab parandada kaasatud osapoolte tööülesannete täitmise efektiivsust ning võimaldab väiksema meeskonnaga teenindada suuremat töötajate hulka, säilitades või isegi tõstes teenuse kvaliteeti.

1.1 Taust ja probleem

Tarkvaraettevõte Bolt Technology OÜ, toonane Taxify, sai tuntuks sõidujagamisplatvormina, mis võimaldas mobiilirakenduse kaudu broneerida taksot selliselt, et enam ei olnud tarvis helistada dispetšerile. Tänaseks tegeleb ettevõte ka autode ja tõukerataste rentimise ning toidukuller teenuse pakkumisega, tegutsedes neljakümnes riigis ja rohkem kui kahesajas erinevas linnas. Algusaegade tagasihoidliku paarikümne töötajaga ettevõttest on tänaseks kasvanud ettevõtte, kus töötab ligikaudu 3000 töötajat.

Ettevõtte algusaegadest saadik on kasutajakonto elutsükli halduse protsess, mis katab töötaja liitmisega, nendega seotud muutuste ja lahkumisega seonduvad toiminguid, olnud manuaalne. Selline protsessi tähendab, et kõik protsessiga seotud meeskonnad on tihtipeale sunnitud oma tööd duplikeerima, mis muuhulgas vähendab töö efektiivsust. Rakenduste ligipääsusid vahendatakse IT meeskonna töötajate poolt käsitsi või kasutatakse veebilehitseja automatsioone. Samuti liigub info ebastandardseid ning aeglaseid kanaleid pidi, sest tihtipeale lähenetakse IT meeskonnale teeninduspileti loomise asemel hoopis Slacki kaudu või defineeritakse tööülesanne lausa suuliselt. Töötajate kiire kasvuga sammu pidamiseks oli tarvis välja mõelda ning rakendada kasvuga skaleeruv kasutajakontode halduse lahendus, vältimaks vajadust IT meeskonna suurust mitmekordselt kasvatada.

1.2 Ülesande püstitus

Käesoleva diplomitöö eesmärgiks on kavandada osaliselt automatiseeritud värbamisprotsess, mis asendaks varasema aja- ja ressursikuluka, ettevõtte kasvuga mitteskaleeruva ning veaohtliku manuaalse protsessi. Uus protsess peaks ettevõttel võimaldama hoida kokku kulusid, suurendada efektiivsust, läbi viia detailsemaid ligipääsude auditeid ja pakkuda lõppkasutajale mugavamat kasutajakogemust. Töös antakse ülevaade kasutajakonto elutsüklist üldiselt, automatiseerimiseks kasutatud tööriistadest, vanast ja uuest protsessist ning ühe rakenduse liidestamisest identiteediteenusega.

Töö ülesanneteks on:

1) Anda teoreetiline taust identiteedi ja ligipääsude halduse valdkonnast
2) Kaardistada kõikidest vaadeldavatest kasutaja elutsüklihalduse protsessidest värbamisprotsess piisava detailsuse astmega
3) Anda ülevaade kasutusel oleva protsessi kitsaskohtadest ning analüüsida optimeerimisvõimalusi vastavas protsessis
4) Optimeerida ning automatiseerida elutsükli protsessi sammud, mis seda võimaldavad

5) Kirjeldada uut protsessi ning näidata selle rakendamist ühe tuumikrakenduse näitel

1.3 Ülevaade tööst

Antud töö praktiline osa on tehtud eesmärgiga aidata töös vaadeldaval ettevõttel oma kasutajate elutsüklihaldusega seonduvaid protsesse optimeerida ja automatiseerida. Käesolev kirjalik töö pakub ülevaadet praktilise töö tulemusena saavutatud protseduurilistest parendustest.

Antud töö jaguneb seitsmeks osaks: sissejuhatus, metoodika, töö teoreetilised alused, esialgne ning täiendatud värbamisprotsessi kirjeldused, ühe tuumikrakenduse liidestamise töökäik ja kokkuvõte. Sissejuhatuses kirjeldatakse lühidalt töös käsitletavat probleemi ning selle tausta. Metoodika kirjeldab rakendatavale protsessile sätestatud nõudeid ning töös kasutatavaid tööriistu. Teoreetiliste aluste peatükis keskendutakse elutsükli mõistele ning identiteedi ja ligipääsude haldusele. Järgnevad kaks peatükki võtavad luubi alla Bolt Technology OÜs varasemalt kasutuses olnud vana ning hiljuti kasutusele võetud uue värbamisprotsessiga seonduva. Töö eelviimases peatükis kirjeldatakse detailselt ühe tuumikrakenduse liidestamise tööprotsessi ning töö lõpetab kokkuvõte.

2 Metoodika

Püstitatud ülesande lahendamiseks kasutab autor IT süsteemide administreerimise õppekava ning Okta sertifikaaditreeningute raames omandatud teadmisi ja töövahendeid. Töö käsitleb nii praktilist osa, mis sai suuresti tehtud juba enne diplomitöö kirjutamist, kui ka teoreetilist osa mis kirjeldab praktilise osa raames tehtud tööd detailselt.

Praktilise töö raames võeti kasutusele identiteedihaldusteenus Okta, mille abil oli võimalik kasutajatele luua tsentraliseeritud kasutajakataloogi identiteet. Identiteeti kasutatakse, et automatiseerida kasutajakonto elutsükli värbamise etapi raames tehtavad IT-, personali- ja värbamismeeskonna ülesanded. Kirjaliku töö raames kirjeldati tehtud praktilist tööd ning kasutati Bizagi Modeler nimelist tarkvara, et visualiseerida töös vaadeldavaid äriprotsesse. Lisaks antakse lugejale teoreetiline taust identiteedi ja ligipääsude halduse ning kasutajakonto elutsükliga seonduvast.

2.1 Bizagi

Töös kirjeldatavate äriprotsesside modelleerimiseks kasutab autor Bizagi Modeler tarkvara. Bizagi Modeler on vabavaraline tarkvara, mis on mõeldud graafiliste protsessidiagrammide koostamiseks ning kasutab BPMN (Business Process Model and Notation) standardit [1]. Selline modelleerimine annab ettevõttele võimaluse mõista oma sisemisi äriprotseduure graafiliste märkide abil ning neid protseduure standardsel viisil erinevate osapooltega jagada.

BPMN on Object Management Group poolt väljatöötatud standardne märgisüsteem, mis kirjeldab äriprotsessi erinevaid sündmusi, tegevusi ja lüüse. Äriprotsesside modelleerimine võimaldab väga erinevate äriprotsessidega seotud informatsiooni edastamist erineva taustaga sihtrühmadele. Ühtse standardi väljatöötamine tagab, et kõik kasutajad koostavad, loevad ja mõistavad mudeleid ühtemoodi, olenemata ettevõtte spetsiifikast või regioonist [2].

2.2 Okta

Töös modelleeritud kasutajakonto elutsükli etappide siseste tegevuste automatiseerimiseks on kasutatud Okta nimelist identiteedihaldusteenust. Okta aitab

ettevõtetel, kus on kasutusel palju erinevaid SaaS tööriistu, mida kõiki tuleb läbi erinevate portaalide hallata, ning kus kogu sellega seonduv halduskoormus hakkab IT meeskonnal üle pea kasvama, lahendada kasutajakonto elutsüklihalduse probleeme. Antud tarkvarateenuse kasutamine võimaldab IT meeskondadel luua kasutajatele digitaalseid identiteete ning neid tsentraalsest kasutajakataloogist hallata. Kasutajakataloog võimaldab identiteediga seotud erinevate atribuutidele tuginedes kasutajad reeglipõhiselt grupeerida. Seeläbi saab omakorda automatiseerida ligipääsuõiguste andmist ja eemaldamist, nii ettevõttes kasutusel olevatesse pilveteenuse põhistesse kui ka ettevõtte sisestesse rakendustesse [3].

Samuti saab luua töövoogusid, mille abil on võimalik kasutajakonto elutsüklihalduse protsesse hõlpsasti automatiseerida. Automatsioone saab luua Okta siseste tegevuste automatiseerimiseks ja ka mistahes avalikult saadaval oleva rakenduse või teenuse API'ga ühendumiseks. Töövoogude ehitamiseks pakutakse graafilist kasutajaliidest mille abil võimaldatakse *if-this-then-that* loogikat kasutades luua mistahes ühendusi [4].

2.3 Nõuded identiteedihaldusteenusele

Töö raames ei keskenduta identiteediplatvorm valimisele ega analüüsita alternatiivseid teenusepakkujaid. Küll aga tuuakse välja nõuded, mille alusel Bolt sobiva identiteedihaldusteenuse valis.

2.3.1 Funktsionaalsed nõuded

Funktsionaalsete nõuete juures keskendutakse sellele, mida peab valitud tarkvara suutma teha. Järgnevalt on loetletud identiteedihaldusteenusele sätestatud funktsionaalsed nõuded.

1. Peab ühilduma ettevõttes kasutatava personalisüsteemiga Workday
2. Peab olema ühilduv väliste kasutajakataloogidega toetamaks allhanke raames palgatavate alltöövõtjate kasutajakontode elutsüklihaldust
3. Kasutajal peab olema Okta kontosse ligipääsu taastamiseks eneseabi võimalus
4. Peab toetama mitmeastmelist autentimist ükskõik millise OTP teenusega
5. Peab olema ühilduv kõikide ettevõtte tuumikrakendustega

6. Peab võimaldama luua kohandatavaid integratsioone rakendustega, millele pole Okta poolt eelintegratsiooni loodud
7. Peab võimaldama kasutajakontosid tsentraalselt ühest kasutajakataloogist hallata
8. Kasutajate ning nendega tehtavad administratiivsed tegevused peavad olema logitavad
9. Peab võimaldama granulaarset ligipääsuõiguste piiramist
10. Peab võimaldama kasutajate grupeerimist reeglite alusel
11. Peab võimaldama ettevõtte standarditele vastavate paroolinõuete seadistamist
12. Peab võimaldama kasutajakonto ja temaga seonduvate andmete täielikku kustutamist
13. Peab võimaldama kasutajakontodega seonduvaid toiminguid ajastada nii kellaajaliselt kui ka kuupäeva järgi

2.3.2 Mittefunktsionaalsed nõuded

Funktsionaalsetest nõuetest rääkides keskendutakse sellele, mida peab valitud tarkvara teha suutma, mittefunktsionaalsete nõuete puhul keskendutakse aga sellele kuidas tarkvara peab vajalikke funktsioone täitma. Järgnevalt käsitletakse identiteedihaldusteenusele sätestatud mittefunktsionaalseid nõudeid.

1. Peab olema mobiilisõbralik
2. Peab ühilduma enimlevinud veebilehitsejatega
3. Peab vastama IT-SEC meeskonna turvanõuetele
4. Kasutajalogid peavad olema filtreeritavad
5. Liidestatud rakendustesse autentimine peab lõppkasutajale mugav olema

2.4 Nõuded uuele loodavale lahendusele

Nõuded loodavale lahendusele aitavad kaardistada, mida uus ja osaliselt automatiseeritud kasutajate elutsüklihalduse protsess võimaldama peaks.

1. Peab eemaldama vajaduse manuaalsete teeninduspiletite loomise järele
2. Peab automatiseerima teavitused protsessiga seotud meeskondade vahel, kui toimuvad elutsükli oleku muutused
3. Peab automatiseerima kasutajakontode loomise ning kustutamise
4. Peab võimaldama kasutajakontodega seonduvate tegevuste ajastamist töövälisele ajale
5. Peab vähendama vajadust palgata uusi IT- ja personalispetsialiste
6. Peab minimeerima kasutajakontode loomisel tehtavaid andmesisestuse vigu
7. Peab võimaldama efektiivset rakenduste litsentside haldamist, võimaldades seeläbi IT kulusid optimeerida

3 Töö teoreetilised alused

Käesoleva töö läbivaks teemaks on kasutajakonto elutsükli haldamine, mistõttu tuleb rääkida ka kasutajakonto elutsüklist üldiselt ning digitaalse identiteedi olemusest. Sealjuures tuleb juttu IT-turvalisuse valdkonnast, mis võimaldab identiteete luua ning nendega seonduvaid tegevusi automatiseerida.

3.1 Kasutajakontode elutsüklihaldus

Me ei saa rääkida ettevõttest mainimata selles töötavaid inimesi. Töötajad on alati pidevas liikumises, neid tuleb juurde ning samas osa neist ka lahkub. Koos töötajate liikumisega tuleb hallata ka nendega seonduvaid kasutajakontosid. Kõikide nende liikumiste üheselt mõistmiseks lepitakse kokku kasutajakonto elutsükli etappides tehtavates toimingutes. Töös vaadeldakse esmalt, mis on erinevad kasutajakonto elutsükli etapid ja mis käivitab muutuse ühest etapist teise ning viimaks vaadeldakse erinevate etappide käigus tehtavaid toiminguid (joonis 1).

Joonis 1. Kasutajakonto elutsükkel

Allikas: https://www.manageengine.com/products/ad-manager/manage-user-life-cycle-in-active-directory

Kasutajakonto elutsüklihaldus kirjeldab töötaja identiteedi kulgemist läbi erinevate elutsükli etappide. Elutsükli peamisteks etappideks on ettevõttega liitumine, selles liikumine ja sellest lahkumine. Kasutaja identiteedi voogu läbi erinevate etappide

nimetatakse kasutaja elutsükli olekute muutuseks. Elutsükli oleku muutuse võivad käivitada näiteks töötaja palkamine, ametikoha muutumine või töötaja vallandamine [5].

Uue töötaja organisatsiooniga liitmise etapi raames peab personalimeeskond personalisüsteemi töötaja jaoks konto looma. Sõltuvalt ettevõttest on juurdepääsu võimaldamine kõigile rakendustele ja kontodele, mida töötaja oma töö tegemiseks vajab, jagatud ülemuste, IT- ja personalimeeskonna vahel. Väiksemates või isegi keskmise suurusega ettevõtetes võib see tunduda triviaalse probleemina. Üha kasvava töötajaskonna ja hallatavate rakenduste arvuga võib aga kiirelt tekkida vajadus hallata väga mitmeid kasutajakontosid arvukates süsteemides [5].

Samuti omandab töötaja oma tööperioodi vältel tihtipeale mitmesuguseid lisanduvaid ligipääse, seda kas tööülesannete muutumise või meeskonnavahetuse järgselt. Juhul kui kasutajale antud ligipääsuõiguste jälgimiseks puudub tsentraalne andmebaas, logi või kataloog, millest oleks võimalik lugeda kõiki kasutajale määratud ligipääse, muutub ligipääsuõiguste eemaldamine väga keerukaks. Töötaja lahkumise sündmuse puhul on pea võimatu tagada olukord, kus kõik kasutajale määratud ligipääsuõigused on eemaldatud, ilma kõiki ettevõttes kasutatavaid rakendusi manuaalselt kontrollimata.

Kasutajakontode elutsüklihalduse probleemide lahendamiseks on võimalik kasutada *Identity and Access Management* ehk identiteedi- ja ligipääsuhalduse süsteeme (IAM). IAM süsteemid võimaldavad ettevõttel automatiseerida ning keskselt hallata kõiki kasutajakonto elutsükli raames ligipääsuõigustega seonduvaid toiminguid. Järgnevas peatükis vaatame lähemalt, mida IAM süsteemid endast kujutavad ja teha võimaldavad.

3.2 Identiteedi ja ligipääsude haldus

Identiteedi- ja ligipääsuhaldus (IAM) on IT-turvalisuse valdkond, mis tegeleb ettevõttesiseste digitaalsete identiteetide haldamise ning neile juurdepääsuõiguste pakkumisega. Seejuures võimaldatakse õigetel inimestel, õigetel põhjustel ning õigel ajal õigetele ressurssidele juurde pääseda [6]. IAM süsteemid pakuvad ettevõtetele tsentraliseeritud tarkvarasüsteeme, mille abil saab identiteetide haldamisega seonduvaid toiminguid automatiseerida ning tagada suurendatud andmete turvalisuse. Identiteedi- ja ligipääsuhalduse süsteemid tegelevad peamiselt kasutaja turvalise autentimise ja autoriseerimisega ning ligipääsude haldamisega [7].

3.2.1 Digitaalne identiteet

Identiteet on teave, mida kasutatakse mingisuguse üksuse või isiku kirjeldamiseks piiritletud süsteemis. Digitaalne identiteet koosneb üldiselt kolmest põhilisest komponendist: unikaalne identifikaator, ligipääsuvõtmed, mille abil ennast tuvastada, ning identiteediga seotud atribuudid [8]. Käesoleva töö raames käsitletakse identiteeti kui töötajaga seonduvat andmeobjekti, mis on talletatud kas IDaaS või HRIS süsteemide siseselt.

3.2.2 IDaaS

Identiteet teenusena (IDaaS) on pilvepõhine autentimisteenus, mille on loonud ja mida haldab kolmas osapool. IDaaS ettevõtted pakuvad oma klientidele pilvepõhist autentimis- ning identiteedihaldamisteenuseid. Pilvepõhise teenuse kasutamise peamine eelis on kulude kokkuhoid, sest puudub vajadus soetada spetsiifilist riistvara ning välja ehitada kohapeal asuvat infrastruktuuri. Samuti puuduvad jooksvad halduskulud ning vajadus palgata riistvara eest vastutavaid spetsialiste [9].

Bolt on oma IDaaS teenusepakkujaks valinud Okta nimelise ettevõtte. Nende identiteediteenus sisaldab kolme suuremat väärtuspakkumist:

- Adaptiivset mitmeastmelist autentimist
- Ühekordset sisselogimist
- Identiteedihaldust

Adaptiivne mitmeastmeline autentimine erineb tavapärasest mitmeastmelisest autentimise (MFA) teenusest selle poolest, et see kogub kasutaja logimise hetkel ka kasutajat kirjeldavaid metaandmeid. Näiteks loetakse sisse kasutaja IP, asukoht ning seade, millelt sessioon alustati. Okta kasutab neid andmeid, et arvutada kasutaja riskifaktor ning vastavalt arvutatud tulemusele otsustada, kas kasutajalt on tarvilik lisanduvat autentimist küsida või mitte. Kui kasutaja logib sisse ettevõtte turvalisest võrgust ei pruugita talt lisanduvat autentimist küsida, küll aga võidakse seda küsida kui kasutaja tundmata võrgust sessiooni alustab [10].

Okta võimaldab ehitada varieeruva astmega ligipääsuõiguseid, mis põhinevad varem arvutatud riskifaktorile. Näiteks võib sensitiivset informatsiooni sisaldavad rakendused teha kättesaadavaks ainult autoriseeritud seadmetest. Sellise turvaeeskirja rakendamisel oleks kasutaja isiklikest seadmetest ühendudes ligipääs rakendusse keelatud [10].

Ühekordne sisselogimine (SSO) on kasutaja autentimise tööriist, mis võimaldab kasutajatel turvaliselt juurde pääseda mitmetele rakendustele ja teenusetele, kasutades ainult ühte kasutajanime ja parooli komplekti. Okta keskkonda logimisel avaneb kasutajale integreeritud rakenduste vaade (joonis 15), mille hulgast valides on võimalik vaid ühe klahvivajutusega sobivale rakendusele ligi pääseda. Töötajatel pole enam tarvis meeles pidada kümneid paroole ning samuti puudub vajadus tööpäeva vältel erinevatesse süsteemidesse sisenemiseks end korduvalt autentida. See säästab töötajate väärtuslikku aega ning lubab neil oma tööülesannete täitmisele keskenduda [11]. Samuti väheneb paroolide taastamiseks kuluv tööaeg.

3.2.3 Identiteedihaldus

Identiteedihaldus on tegevus identiteedi ja juurdepääsu haldamise funktsioonis, mis käsitleb kasutaja unikaalset digitaalset esitust, sealhulgas kõigi sellega seotud atribuutide ja õiguste talletamist ning haldamist [12]. Identiteete saab luua IAM süsteemi siseselt, kuid neid on võimalik ka välistest kasutajakataloogidest (näiteks Windows AD, Workday) importida, eeldusel, et välise kasutajakataloogi ja IAM süsteemi vahele on vastav integratsioon loodud, identiteedi profiilid seadistatud ning atribuudid kaardistatud.

Iga IAM süsteemi selgrooks on võimekas identiteedikataloog. Identiteedikataloogid pakuvad võimalust identiteediga seotud andmete turvaliseks salvestamiseks ja korrastamiseks. Kataloogid talletavad ja haldavad identiteetide atribuute, pakkudes

sealjuures võimalusi identiteetide juurdepääsupoliitikate loomiseks ning turvalisuse tagamiseks.

Okta kasutab oma identiteedikataloogina Okta Universal Directory nimelist kataloogi. Universaalse kataloogi (Okta Universal Directory) universaalsus väljendub võimekuses talletada piiramatul arvul identiteete ning nendega seotud atribuute, mis pärinevad kas IAM süsteemiga integreeritud rakendustest või välistest kasutajakataloogidest AD, HRIS, CRM, või ERP [13],[14]. Samuti võimaldatakse identiteete luua ükshaaval otse kataloogis või CSV'd , kui korraga on tarvis luua mitmeid identiteete. Okta identiteedikataloog koondab kõik kasutajad, olenemata nende profiili esialgsest päritolust, ühte peakataloogi ning lubab neid gruppidesse lisada kas manuaalselt või grupireegleid kasutades [14].

Bolt kasutab töötajate identiteetide loomiseks lähenemist, kus personalisüsteem on IAM süsteemile ülemsüsteem. Töötaja identiteedi loomine toimub kasutajaandmete importimisel personalisüsteemist IAM süsteemi. Personalisüsteemist loetakse kaasa üle 30 erineva atribuudi, mida regulaarsete sünkroonimiste käigus kahe süsteemi vahel ajakohasena hoitakse. IAM süsteem võimaldab loodud identiteedile samuti unikaalseid atribuute juurde lisada, mida on soovi korral võimalik ka ülemsüsteemi sünkroniseerida.

3.2.4 Ligipääsuhaldus

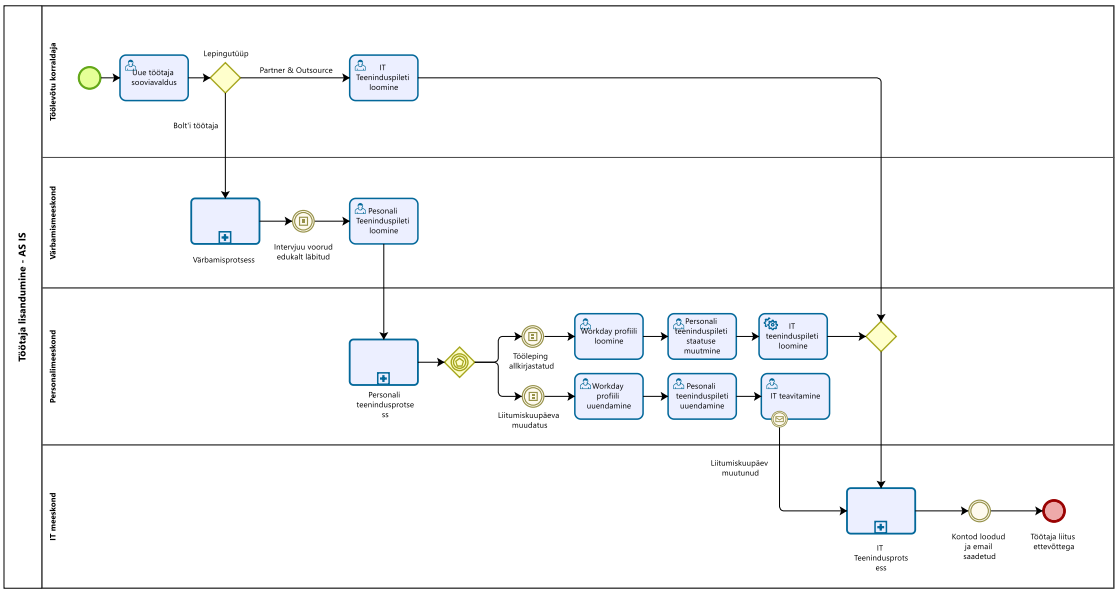
Ligipääsuhaldus on protsess, mille käigus antakse volitatud kasutajatele õigused teenuse või rakenduse kasutamiseks, piirates samaaegselt juurdepääsu volitamata kasutajatele. See on üles ehitatud võimel volitatud kasutaja identiteeti täpselt tuvastada ning seejärel hallata tema juurdepääsu teenustele, tuginedes identiteediga seotud atribuutidele, näiteks organisatsioonilisele rollile või tööfunktsioonile. Ligipääsuhalduse poliitikate tõhus elluviimine aitab turvata ettevõtte andmeid ja intellektuaalomandit. Ligipääsuhaldus on tõhus infoturbehalduse poliitikate ning eeskirjade rakendamine ent selle raames ei otsustata, kellel millisele IT-teenusele juurdepääs olema peaks. Niipea kui kasutaja on autenditud ning piisav ligipääsuõigus tuvastatud, antakse talle õigused taotletud rakenduse või teenuse kasutamiseks [15].

4 Värbamisprotsess AS-IS

Käesolevas peatükis keskendutakse olemasoleva manuaalse kasutaja elutsüklihalduse protsessi kirjeldamisele ning kaardistamisele. Järgneva alapeatüki raames on välja toodud elutsükli etapi sammud ning sellega seotud osapooled. Olukorra kaardistamisel on autor põhinenud enda töökogemusele, mis hõlmab endas vastava protsessi tehnilist rakendamist ning koostööd erinevate protsessi kuuluvate meeskondadega.

4.1 Värbamisprotsessi üldine kirjeldus

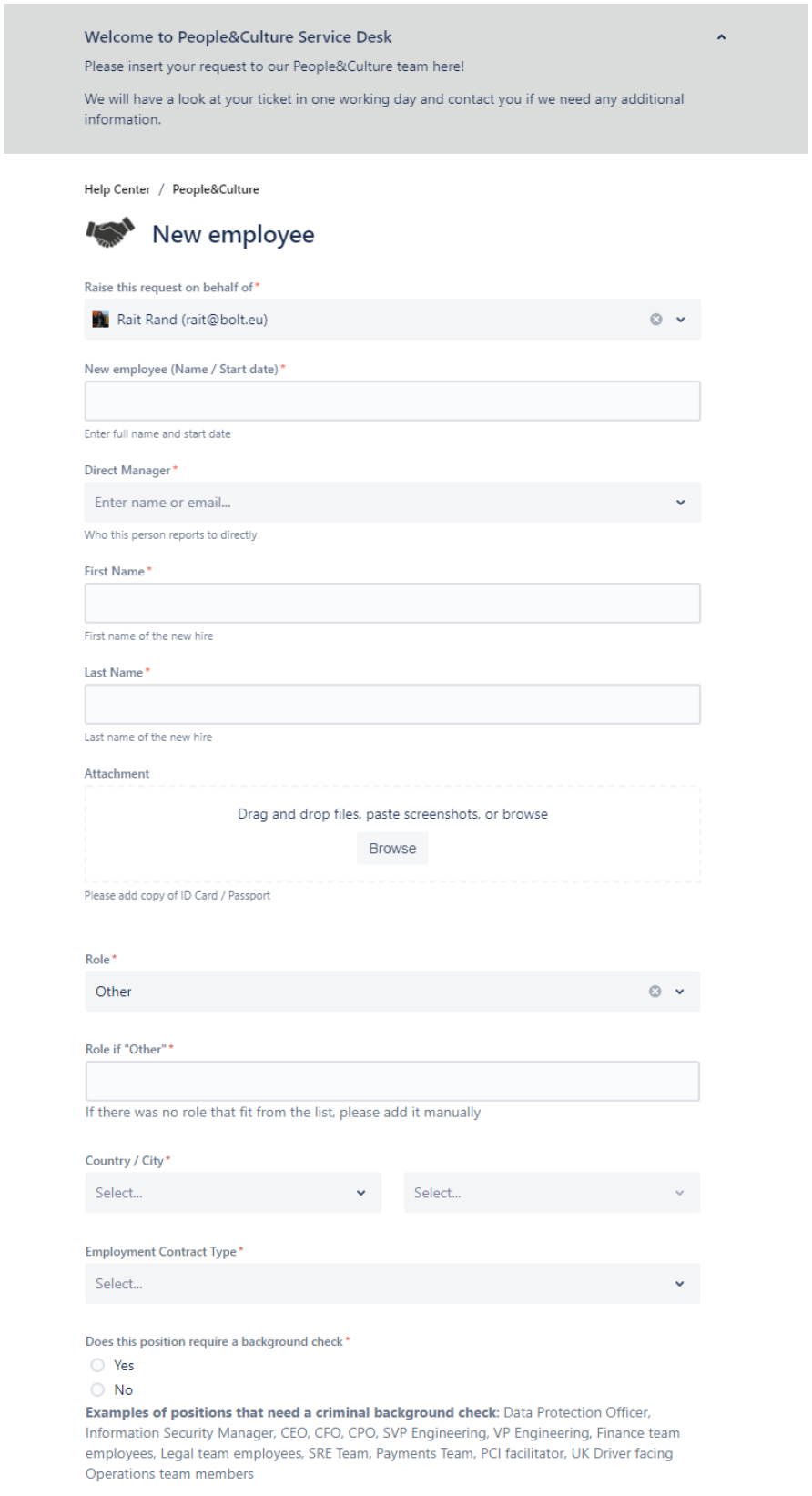
Käesoleva alapeatüki raames antakse ülevaade olemasolevast värbamisprotsessist. Vastav protsess on kujutatud joonisel 2.



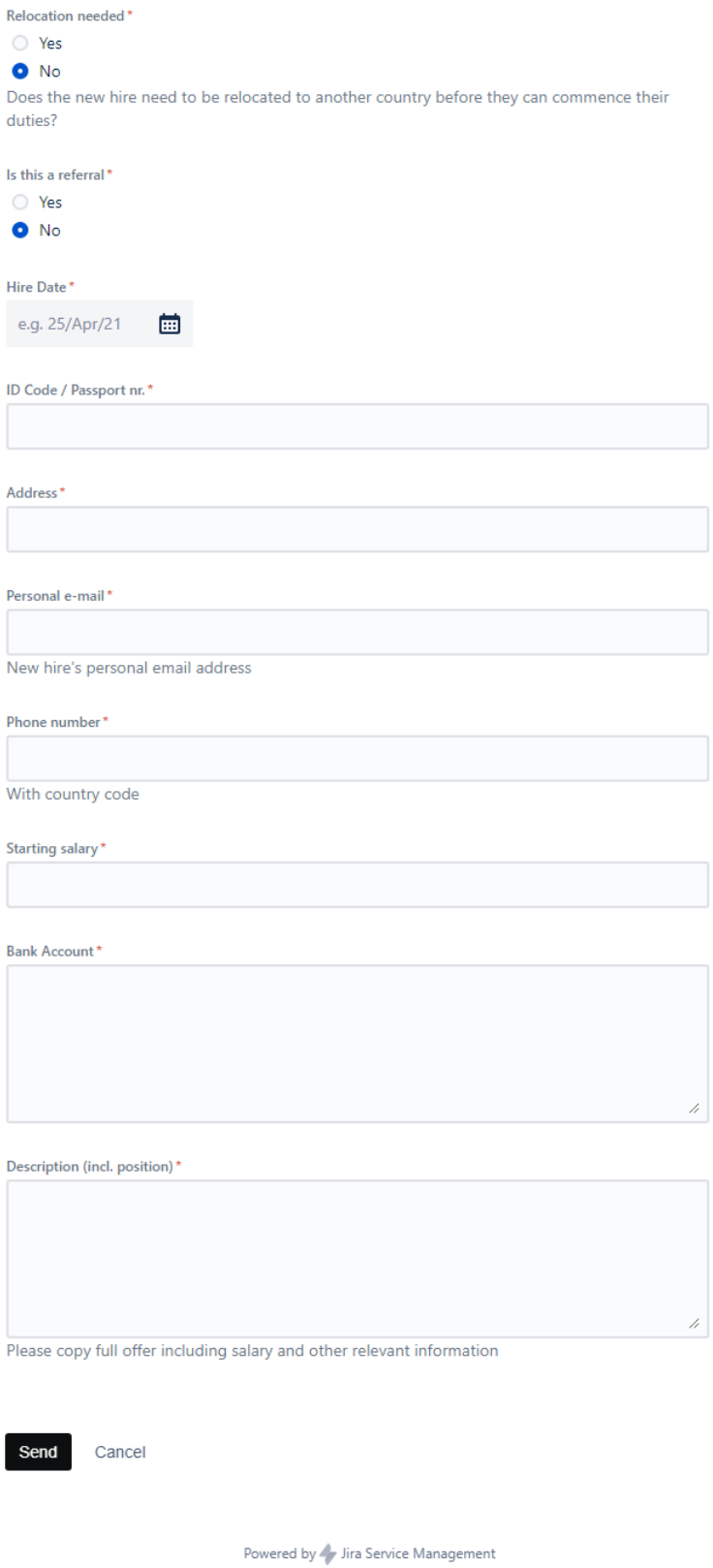
Joonis 2. Töötaja värbamisprotsess AS-IS

Protsess algab töölevõtu korraldaja soovist uut inimest palgata. Olenevalt lepingutüübist hargneb protsess kaheks. Juhul, kui soovitakse palgata partnerluslepinguga töötajat või alltöövõtjat, tuleb töölevõtu korraldajal luua pilet otse läbi IT meeskonna Service Desk portaali. Kui aga on vaja palgata Bolt'i töötaja, siis tuleb kontakteeruda värbajatega, kes alustavad värbamisprotsessiga ning leiavad varasemalt defineeritud kriteeriumitele

vastava kandidaadi. Sobiva kandidaadi leidmisel ning intervjuuvoorude edukal läbimisel loovad värbajad personalimeeskonnale pileti, mis sisaldab tulevase töötaja andmeid:



Joonis 3. Personalimeeskonna uue töötaja andmete vorm



Joonis 4. Personalimeeskonna uue töötaja andmete vorm

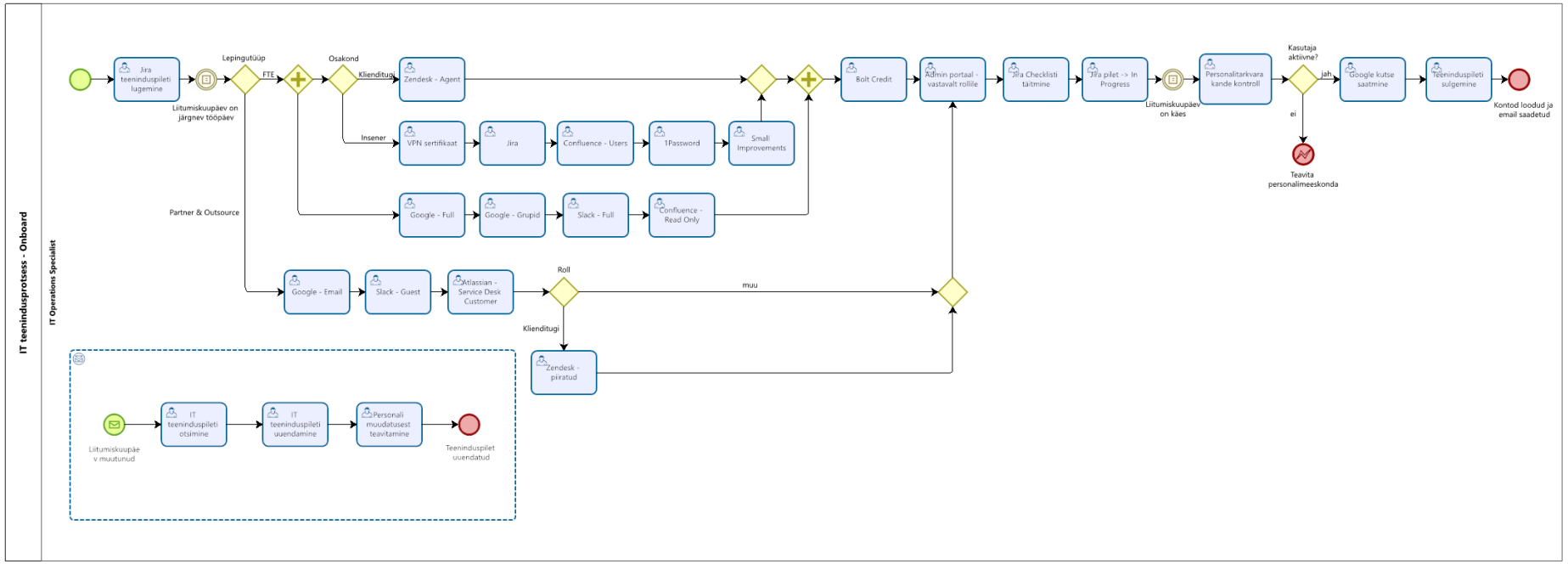
Personalimeeskonna teeninduspileti loomiseks kasutatav vorm, mis täidetakse uue töötaja värbamiseks, koosneb minimaalselt kahekümnest erinevast väljast. Eelmainitud vorm on kujutatud joonisel 3 ja joonisel 4. Täidetava vormi mahukuse tõttu on sellisel kujul teeninduspiletite loomine väga aeganõudev tegevus. Eriti ajakulukaks osutub see olukorras, kus palgatakse rohkem kui üks töötaja korraga. Lisaks tuleb arvesse võtta fakti, et väljade täitmine toimub manuaalselt, mistõttu esineb andmetes tihtipeale trükivigu.

Pileti loomisega algab personalimeeskonna teenindusprotsess, mille raames koostatakse muuhulgas ka leping ning kantakse uus töötaja HRIS süsteemi. Pärast personalisüsteemi Workday sissekannet ning pärast töölepingu allkirjastamist uuendatakse personalispetsialisti poolt Service Desk'is asuva pilet *in progress* staatusesse, mis omakorda käivitab Atlassian'i automatsiooni ning loob personalimeeskonna pileti põhjal IT meeskonnale teeninduspileti. Loodud piletilt on eemaldatud tundliku sisuga väljad, mida IT meeskonna ülesannete edukaks lahendamiseks tarvis ei ole - isikukood, palgainfo, arveldusarve jms. IT teenindusprotsessi vaadeldakse edaspidi juba lähemalt.

Olukorras, kus IT pilet on juba loodud kuid pärast seda toimub kasutaja liitumiskuupäeva muudatus, ning personalimeeskond muudab enda projekti teeninduspileti sisu, ei kajastu vastav muudatus IT meeskonna piletil. Seetõttu tuleb lisanduva sammuna personalispetsialistil IT meeskonda kas emaili või Slack'i teel muudatusest teavitada. Seejärel peab keegi IT meeskonnast vastava muudatuse konkreetse töötajaga seotud teeninduspiletil manuaalselt sisse viima. Sellise lahenduse puhul aga on lihtne tekkima infosulg või unustatakse lihtsalt vajalikud muudatused sisse viia.

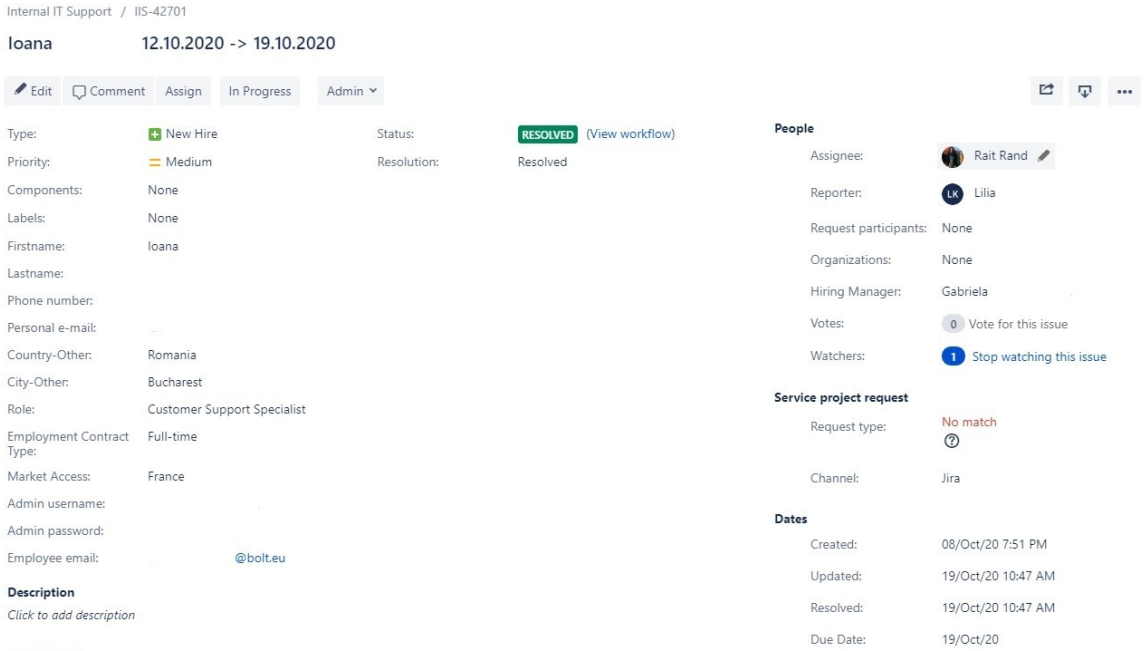
4.2 IT teenindusprotsessi kirjeldus

IT protsessi raames luuakse alustavale töötajale kõik tööks vajalikud kontod ning rakenduste ligipääsud. Joonisel 5 on näha detailselt kaardistatud IT teenindusprotsess.



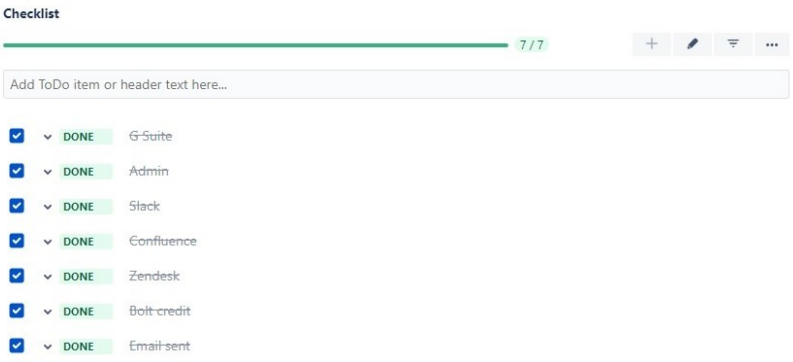
Joonis 5. IT meeskonna teeninduprotsess AS IS

IT protsess algab teeninduspileti (joonis 6) lugemisega ning juhul, kui piletis märgitud palkamiskuupäev on võrdne järgneva tööpäevaga, alustab IT-spetsialist kontode manuaalset ettevalmistamist.



Joonis 6. IT meeskonna teeninduspilet

Pärast kontode loomist täidab IT spetsialist pileti küljes oleva kontollnimekirja (joonis 7), märkides *done* tähisega kontod, mis loodi, ning *skipped* tähisega kontod, mida ei olnud tarvis või ei olnud mingisugusel põhjusel võimalik luua. Kui kontollnimekiri on täidetud, muudetakse teeninduspileti *in progress* staatusesse ning jäädakse liitumiskuupäeva ootama.



Joonis 7. IT meeskonna teeninduspileti kontrollnimekiri

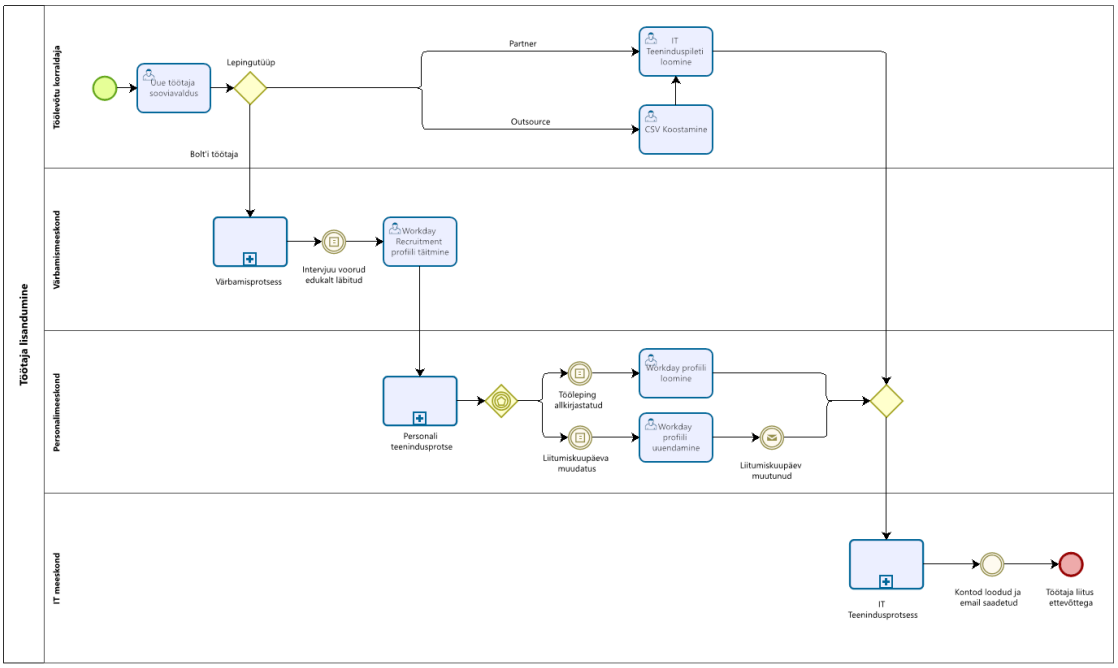
Palkamiskuupäeva kätte jõudmisel tehakse manuaalne kontroll personalisüsteemi, kontrollimaks, kas töötajaprofiil on aktiivne või mitte. Kui peaks selguma, et personalisüsteemi Workday pole töötaja kohta kannet tehtud, tuleb personalimeeskonda sellest teavitada ning jõuda selgusele, miks antud viga tekkinud on (näiteks on muutunud alustamiskuupäev, personalimeeskond on unustanud kasutaja kande teha vms). Aktiivse kasutaja staatuse puhul viiakse läbi protsessi viimane samm ning saadetakse välja Google konto kutse kasutaja isiklikule emailiaadressile. Selline protsess aga muudab keeruliseks iga uue nädala ning kuu algused, kuhu on planeeritud suur kogus uusi värbamisi. Seeläbi tekib nn pudelikael, kus IT-spetsialistid võivad kulutada tunde värbamisülesannete lõpetamiseks ning kutsete välja saatmiseks.

5 Värbamisprotsess TO-BE

Antud peatükis keskendutakse uue, osaliselt automatiseeritud töötaja värbamisprotsessi kaardistamisele ning kirjeldamisele. Peatükis on samuti visualiseeritud uus värbamisprotsessi mudel, kust ilmneb, et varasemaga võrreldes on samme jäänud vähemaks. Kirjeldatakse kuidas identiteeditenust Okta on protsessi automatiseerimiseks ning optimeerimiseks rakendatud.

5.1 Värbamisprotsessi üldine kirjeldus

Üldjoones sarnaneb uue protsessi mudel varasemale protsessile, kuid erineb siiski mitme võtmeteguri poolest (joonis 8). Just nendele võtmetegurite edaspidi keskendutaksegi.



Joonis 8. Värbamisprotsess TO-BE

Märgatavalt on vähenenud manuaalselt tehtava töö maht. Esimese näitena võib tuua teeninduspiletid, mida oli varasemalt tarvis luua alltöövõtjate palkamiseks ning mille arvukus võis kiirematel nädalatel küündida üle saja. Mainitud teeninduspileteid loodi varasemalt käsitsi ning ühekaupa, kuid tänu uuele protsessile pole neid enam tarvis manuaalselt luua. Selle asemel täidab allhanke ettevõtte töölevõtu korraldaja Bolt'i IT

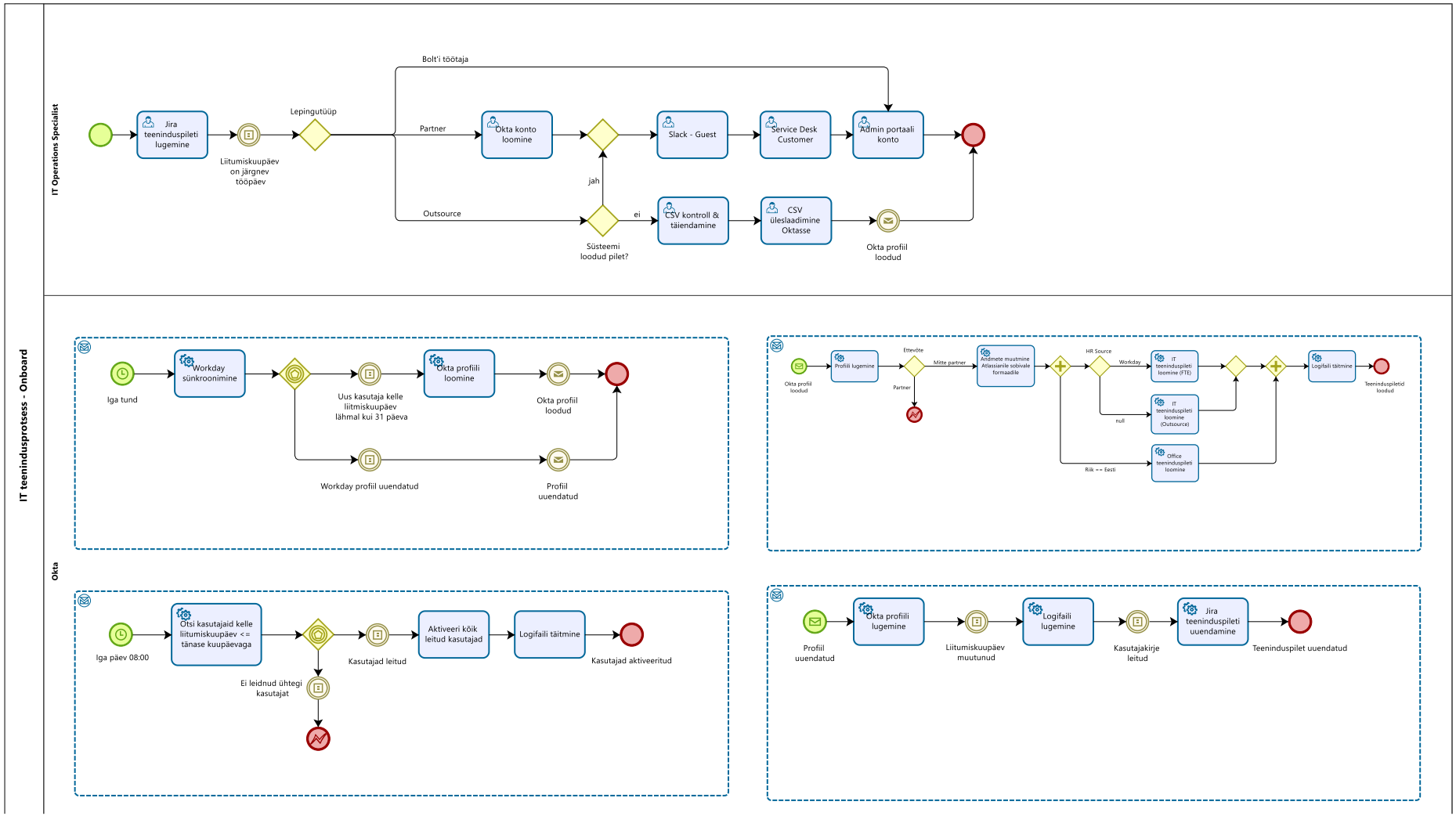
meeskonna poolt loodud CSV faili põhja ning lisab sinna järgmisel nädalal alustavate töötajate informatsiooni, mille edastab ühe teeninduspiletina.

Sarnaseid täiendusi on tehtud ka Bolt'i täiskohaga töötajate värbamise protsessis. Enam pole tarvis värbajatel ega personalimeeskonnal Jira Service Desk keskkonnas töötada. Teeniduspiletite asemel on kasutusele võetud Workday Recruiting nimeline rakendus. Rakendus võimaldab värbajatel hallata tervet värbamismeeskonna sisest protsessi algusest lõpuni. Sobiva kandidaadi leidmisel on võimalik tulevase töötaja eeltäidetud profiil kanda otse personalisüsteemi, kaotades ära vajaduse luua teeninduspilet.

Lisaks eelmainitule on ka ära kadunud vajadus personalimeeskonna teenindusprotsessi siseselt toimunud muudatustest IT meeskonda eraldi teavitada. Näiteks juhul, kui töötaja liitumiskuupäev peaks muutuma, on varasema Slacki või emaili teavituse asemel vaja muudatus vaid HRIS süsteemi kanda. Sealt edasi liigub informatsioon juba automatiseeritud kanaleid pidi, mida töös ka hiljem käsitletakse.

5.2 IT teenindusprotsessi kirjeldus

Teiste värbamisprotsessiga seotud meeskondade jaoks tõi täiustatud protsess kaasa väiksema ajakulu, kuid IT meeskonna jaoks peaaegu täieliku protsessi muudatuse, mis ei väljendunud mitte ainult vähenenud ajakulus vaid ka suurenenud turvalisuses ja kulude kokkuhoius. Protsessi optimeerimiseks võeti kasutusele uus tööriist, Okta, mis pakub kasutajatele digitaalset identiteeti. Olenevalt töötaja lepingutüübist on protsess pea täielikult või vähemalt osaliselt automatiseeritud. Võrreldes joonisel 5 olevat protsessi joonisel 9 oleva protsessiga on selgelt näha, et muutusi on palju, mistõttu vaatame järgnevalt iga alamprotsessi ka lähemalt.

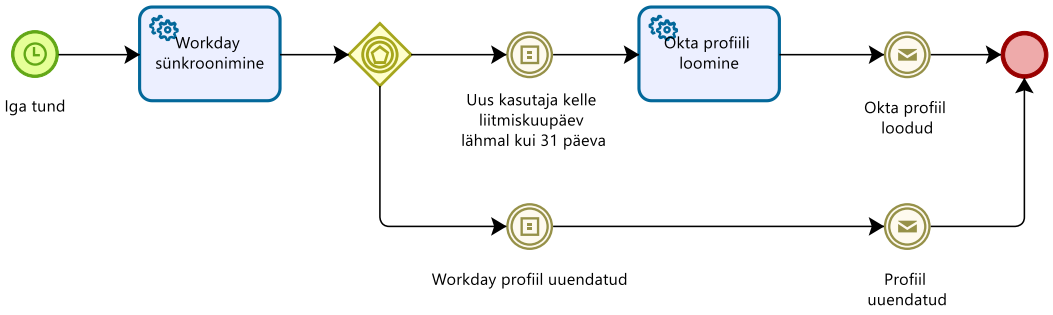


Joonis 9. IT meeskonna teenindusprotsess TO-BE

5.2.1 Kasutajakataloogi sünkroonimine

Selleks, et IT meeskond üldse mingeid automatsioone saaks ehitada, on tarvis keskset kasutajate kataloogi. Nagu eelpool mainitud, pakub Okta selleks Universal Directory nimelist teenust, kuhu on võimalik erinevatest algsüsteemidest kasutajaid sisse laadida. Bolt'i näitel on liidestus tehtud Workday nimelise HRIS süsteemiga, millega toimub sünkroniseerimine iga tunni tagant. Sünkroniseerimise käigus loetakse sisse kõik Workday poolel loodud kasutajad ning nendega tehtud muudatused (joonis 10).

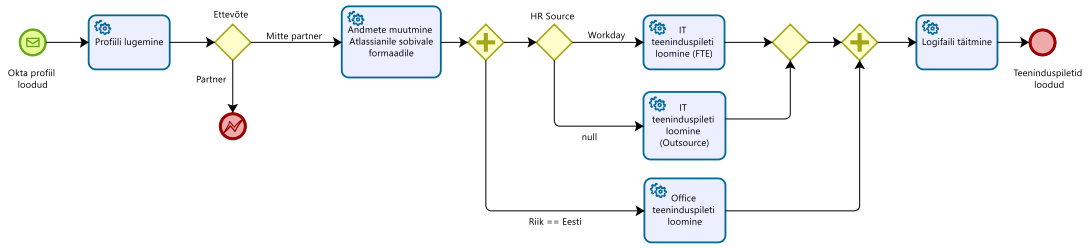
Juhul, kui leitakse kasutaja kelle liitumiskuupäev on lähemal kui 31 päeva ning ta kohta puudub Okta kasutajakataloogis sissekanne, imporditakse kasutaja koos kõikide oma atribuutidega Okta keskkonda. Atribuudid, mida on üle kolmekümne, on varasema Okta ning Workday liidestuse käigus defineeritud. Okta keskkonda importimisel luuakse kasutajale identiteet ning proovitakse kasutajat ka koheselt grupireeglite põhjal erinevate gruppide liikmeskonda lisada. Gruppe kasutatakse erinevate tööks vajalike rakenduste ligipääsude automaatseks vahendamiseks.



Joonis 10. Töövoog - Workday sünkroonimine

5.2.2 Teeninduspiletite loomise töövoog

Siiski eksisteerib rakendusi mida pole võimalik Oktaga üldse või täielikult liidestada, mistõttu on IT meeskonnal endiselt vaja teeninduspileteid ka Bolt'i oma töötajate kohta, mille põhjal kasutajale Okta poolt vahendamata rakenduste ligipääs manuaalselt lisada. Samuti luuakse IT meeskonnale pileteid manuaalselt partnerite ning alltöövõtjate CSV edastamise tarvis, seetõttu sai Oktasse loodud järgnev töövoog, mis on kujutatud joonisel 11.



Joonis 11. Töövoog - teeninduspiletite loomine

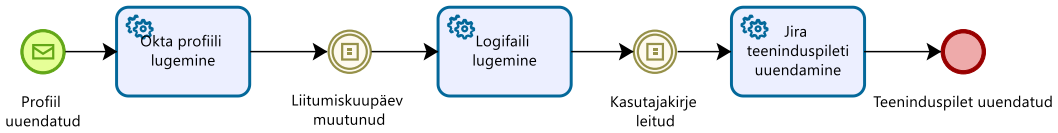
Töövöög algab Okta profiili loomise sündmusega, seejärel loetakse sisse profiilil leiduvad atribuudid. Juhul, kui tegu on partneriga, väljutakse töövoost veateatega ning alamprotsessiga ei jätkata. Muul juhul muudetakse Okta profiilil olevad atribuudid Jira Service Desk pileti loomiseks tarvilikku formaati. Okta profiili algallika ning riigi atribuudi põhjal langetatakse otsus, millistele meeskondadele on teeninduspileti loomine vajalik. Näiteks kui tegu on Eestis alustava töötajaga, luuakse lisaks IT meeskonnale teeninduspilet ka kontorihaldustiimile, mille sisuks on kontori tööpinna ning turvakaardi ettevalmistamine. Kui teeninduspileti loomisel probleeme ei esinenud, kantakse ka vastav kirje logifaili.

5.2.3 Teeninduspiletite uuendamise töövoog

Kui eelmises sammus sai teeninduspilet loodud, võib see IT Service Desk projektis oma täideviimist oodata kuni 31 päeva. See on võrdlemisi pikk aeg ning selle aja jooksul võib juhtuda, et töötaja alustamise kuupäeva muudetakse. See info on IT meeskonnale kriitilise tähtsusega, vältimaks olukorda, kus kasutajale on ligipääsud vääralt väljastatud või hoopis andmata jäänud. Näiteks võib tekkida olukord, kus ligipääsud on väljastatud enne, kui töötaja on ettevõttes tööle asunud, või on töötaja tublisti kontoris kohal, kuid peab oma ligipääse mitu tundi ootama kuna IT meeskonnal puudus informatsioon, et töötaja just sellel päeval liitumas on.

Eelmainitud olukordade vältimiseks lõi autor Okta töövoo, mille abil on võimalik automaatselt Jira Service Desk teeninduspileti liitumiskuupäeva uuendada (joonis 12). Automatsioon käivitub kui toimub Okta profiili uuendamise sündmus, mille saadab välja iga tunni tagant toimuv Workday sünkroniseerimise töövoog, nagu on kujutatud joonisel 10. Juhul kui profiilil muudetud väljade hulgas oli ka liitumiskuupäeva atribuut, loetakse eelnevas sammus täidetavat logifaili, kuhu on muuhulgas salvestatud ka loodud piletite unikaalsed tähised. Kasutajakirje edukal leidmisel saadab Okta Atlassian'i API *endpoint*

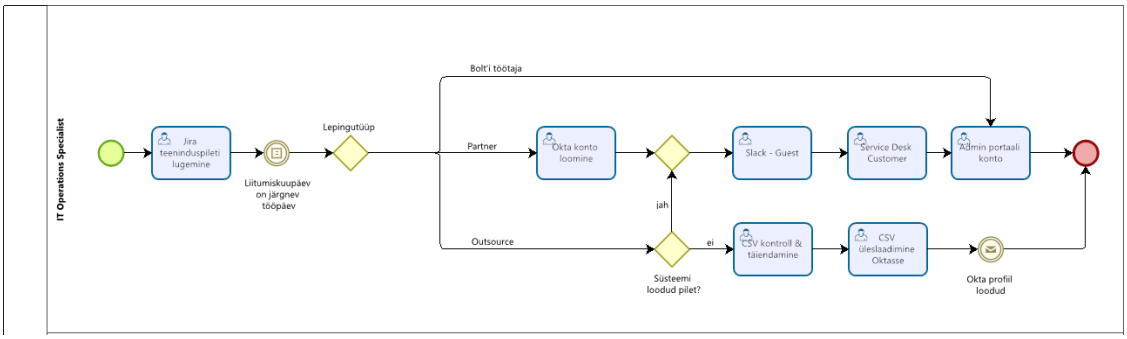
pihta *PUT* päringu, mille sisuks on teeninduspileti pealkiri ja liitumiskuupäeva väli uuendada.



Joonis 12. Töövoog - teeninduspileti uuendamine

5.2.4 IT spetsialisti ülesanded

Kuigi Okta on suure osa kasutajakontode loomisega seonduvast koormusest eemaldanud on siiski protsessis samme, kus IT spetsialisti sisend on vajalik (joonis 13). Uue töötaja liitumiskuupäevale eelneval tööpäeval avab IT spetsialist teeninduspileti ja loeb piletile lisatud kontrollnimekirjalt, milliseid kontosid on tarvis luua. Juhul kui tegu on Bolt'i töötajaga piisab meie ettevõtte sisese Admin portaali konto loomisest. Partnerite ja alltöövõtjatega on siiski mõnevõrra rohkem samme.



Joonis 13. IT spetsialisti manuaalsed tegevused

Allhanke puhul tuleb esmalt vaadata, kas teeninduspilet on loodud süsteemi poolt ühe kasutaja kohta või on tegu teeninduspiletiga, mis sisaldab CSV faili järgneva nädala kõikidest liitujatest. Teisel juhul tuleb CSV fail üle kontrollida ning vajadusel seda täiendada. Kui IT spetsialist CSV sisuga rahule jääb, impordib ta selle Oktasse, kus omakorda luuakse iga CSV rea kohta eraldi Okta profiil. Okta profiili loomine käivitab joonisel 11 kirjeldatud töövoo ning loob iga kasutaja kohta eraldi teeninduspileti.

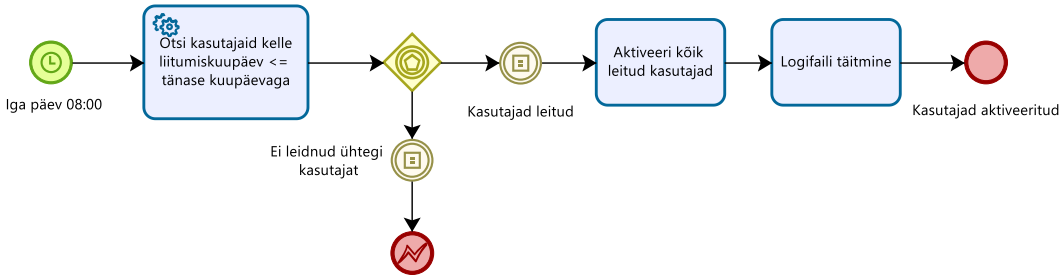
Vastav protseduuriline muudatus sai tehtud, sest kohati pidi kuni 100 kasutaja kohta joonisel 3 ja joonisel 4 ja kuvatud vormi täitma, mille eest vastutas allhanke ettevõtte

töölevõtu korraldaja. Samuti võidab sellest ka IT meeskond, sest enam pole vaja iga alltöövõtja kohta Okta profiili manuaalselt luua. Individuaalsete partnerite ja alltöövõtjatest töötajatega seonduvate teeninduspiletite lahendamine toimib varasema protsessiga võrdlemisi sarnaselt. Endiselt on tarvis luua limiteeritud ligipääsuga Slack, Service Desk külaliskonto ja Admin portaali konto.

5.2.5 Kasutajakontode aktiveerimise töövoog

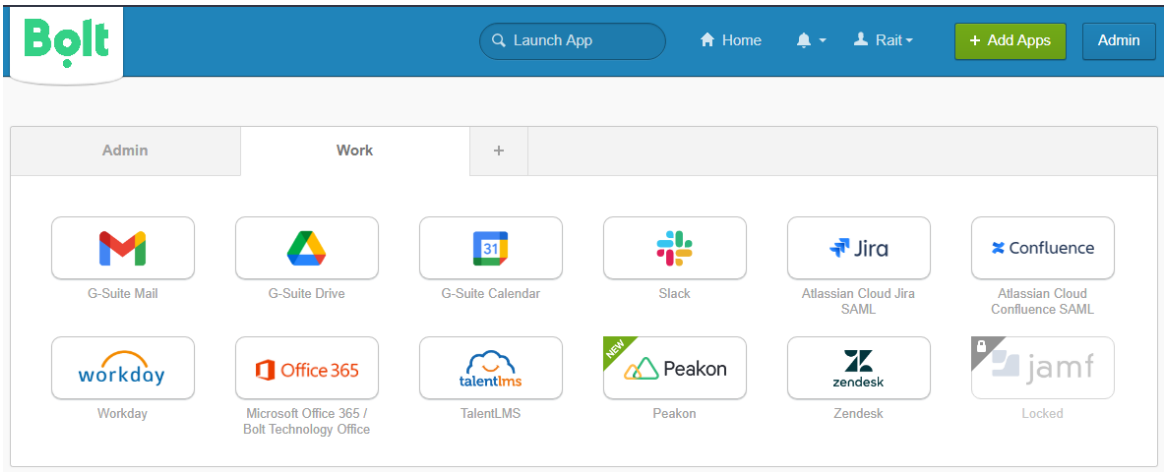
Samuti on loodud töövoog, mis automatiseerib Okta kasutajakontode aktiveerimise (joonis 14). Iga hommik kell 8 otsib Okta kasutajaid, kes on *staged* staatuses ning kelle liitumiskuupäev on möödas või võrdne tänase kuupäevaga. Kasutaja leidmisel aktiveeritakse tema Okta konto, mis omakorda saadab kasutaja isiklikule emailiaadressile konto aktiveerimise lingi.

Vastava töövooga lahendatakse ära varasemalt mainitud probleem, kus töötajate palkamisülesanded kuhjusid uue nädala või kuu algusesse. Samuti võimaldab see planeerida kasutajate aktiveerimisi töövälisele ajale.



Joonis 14. Töövoog - kasutajakontode aktiveerimine

Okta konto aktiveerimisel ja kaheastmelise autentimise ülesseadmisel avaneb kasutajale joonisel 15 nähtav rakenduste vaade. Kasutaja saab Okta rakenduste paneeli kasutades ühe klahvivajutusega pea kõikidele oma kontodele mugavalt ligi. Siinjuures tuleks ka märkida, et kasutaja ei pea enam kuvatud rakenduste tarvis uusi paroole looma ega rakendusi eraldi emaililingi kaudu aktiveerima.



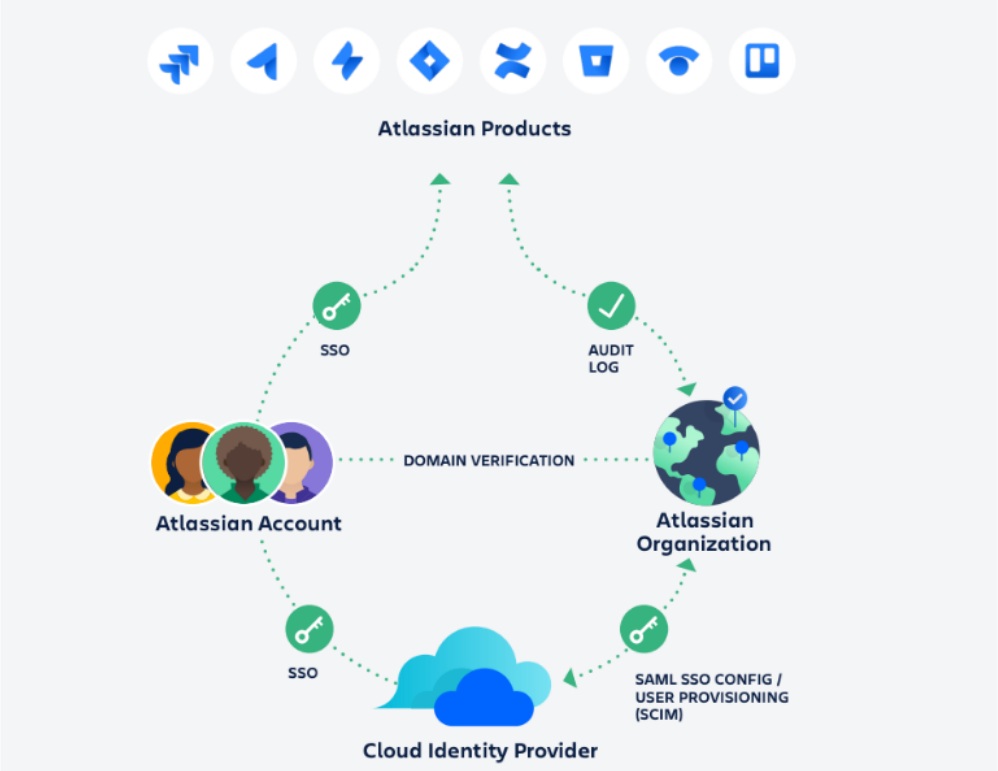
Joonis 15. Okta rakenduste vaade

6 Atlassian Cloud liidestamine Oktaga

Selleks, et anda ülevaade tööst, mis uue värbamisega seotud protsessi rakendamise tarvis tehti, kirjeldab autor järgnevalt ühe tuumikrakenduse liidestamise töökäiku. Kõnealuseks rakenduseks on Atlassian Cloud, mis hõlmab endas järgnevaid Atlassian'i produkte: Jira, Confluence ja Service Desk. Atlassian Cloud on Okta Integration Network kataloogist kättesaadav rakendus, kuid pelgalt selle Oktasse lisamine pole liidestuse toimimiseks kaugeltki piisav.

6.1 Atlassian Access

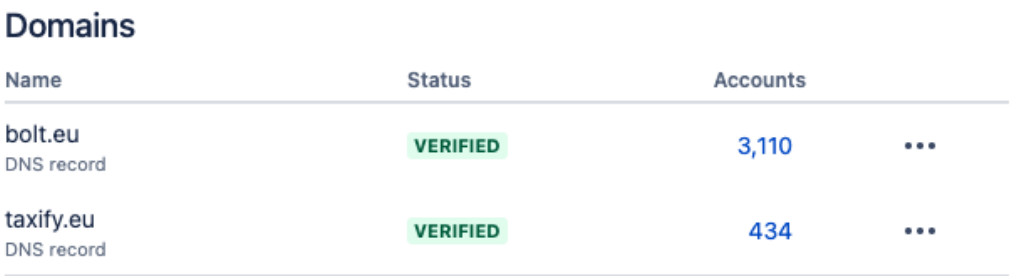
Nagu töös eelnevalt mainitud, kasutatakse kasutajate automaatseks provisioneerimiseks Oktat. Selleks on tarvis kasutada Atlassian Access'i lisamoodulit, mis aga vaikimisi kättesaadav ei ole. Sellele ligipääsu saamiseks soetati aastane tellimus, maksumusega 40000 eurot [16]. Atlassian Access lisab Atlassiani tootele võimekuse toetada SSO'd, automaatset kasutajate provisioneerimist ja pakub ka detailset auditeerimislogi joonis 16) [17].



Joonis 16. Atlassian Access

Allikas: https://www.atlassian.com/software/access/guide/overview#who-should-use-access

Atlassian Access mooduli soetamine võimaldab administraatoril Atlassian'i organisatsiooni alt ettevõtte kasutuses olevad domeenid verifitseerida ning seeläbi kõiki oma töötajaid ühe organisatsiooni alt keskselt hallata. Domeenide taxify.eu ja bolt.eu verifitseerimiseks saadeti Atlassiani poolt väljastatud TXT kirje SRE meeskonnale, et nad selle Bolt'i nimeserveri kirjete alla kanda saaksid.



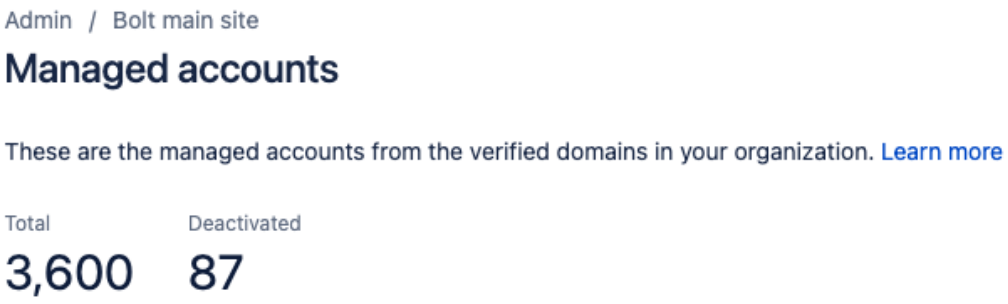
Joonis 17. Atlassian'i verifitseeritud domeenid

Domeenide edukal verifitseerimisel täidetakse Atlassian'i administraatorpaneeli all asuv kasutajakataloog kasutajatega, kellel on ükskõik millise Atlassian'i saidi ning ükskõik millise Atlassian'i toote ligipääs. Seda eeldusel, et nende kasutajakontod on registreeritud kasutades ühte kahest varasemalt verifitseeritud domeenist. Kasutajakataloogi sirvides ilmnes kaks suurt probleemi:

- Palju sulgemata kontosid, millega pole pikka aega sisse logitud
- Ühele kasutajale kuuluvad duplikaatkontod, mis on registreeritud nii taxify.eu kui ka bolt.eu domeeniga

6.2 Kasutajabaasi puhastamine

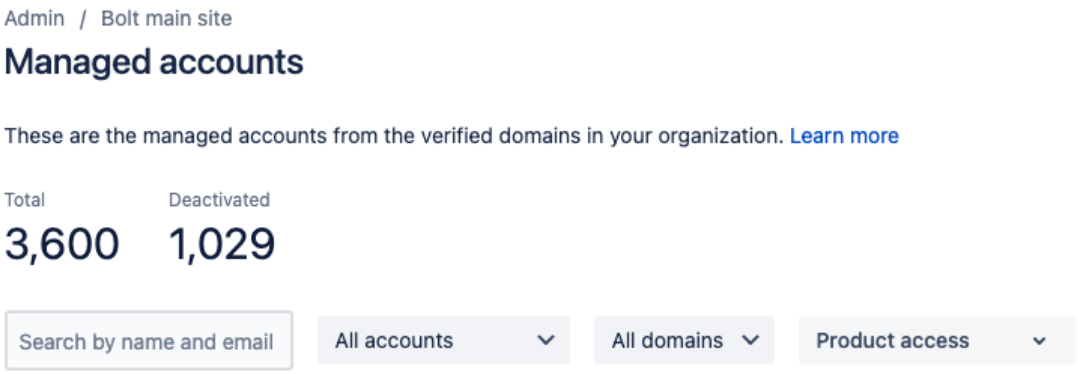
Käesolev alapeatükk käsitleb eelmainitud probleemide lahendamist, mis on eelduseks automaatse provisioneerimise rakendamiseks. Sulgemata kontode probleemiga tegelemiseks otsustati sulgeda kõik kontod, mida pole alatest 2020. aasta algusest kasutatud. Joonis 18 kuvab kasutajakataloogi olukorda pärast domeenide verifitseerimist, kui pole veel tehtud kasutajabaasi puhastamist.



Joonis 18. Atlassian'i kasutajakataloog enne kasutajate deaktiveerimist

Atlassian'i administraatorpaneeli kasutajaliides ei võimalda efektiivselt kasutajakontosid hulgi sulgeda, mistõttu tuli koostada deaktiveerimist vajavatest kasutajatest koosnev CSV fail ning kirjutada skript, vt. Lisa 2. Skript loeb sisendina CSV faili kuhu on märgitud Atlassian'i kasutaja unikaalne identifikaator, kasutajanimi ning email. Järgnevalt saadetakse iga CSV rea kohta Atlassian'i API *endpoint* pihta *POST* päringu, mille sisuks on kasutajakonto sulgeda [18]. Seejärel vaadatakse, kas päring oli edukas või mitte, ning vastused logitakse logifailidesse.

Skripti abil suleti kokku 942 aktiivset Atlassian'i kasutajakontot (joonis 19). Siinkohal tuleks täpsustada, et varasemalt avatuks jäänud kontod ettevõttele mingisugust turvariski ei kujutanud. Atlassian'i kontodesse ei olnud võimalik logida kasutajanime ja parooli kombinatsiooniga vaid läbi Google SSO. Google konto aga suleti töölt lahkumise või vallandamise järel eranditult iga kord. Kontode sulgemise peamiseks eesmärgiks oli Atlassian Access teenuse kulude optimeerimine ning üldine kasutajabaasi puhastus. Ühe kasutaja litsents maksis ettevõttele 1.11€ kuus, ehk ainuüksi Atlassian Access tasude optimeerimise pealt võimaldati ettevõttel säästa 12 547€ aastas [16].



Joonis 19. Atlassian'i kasutajakataloog pärast kasutajate deaktiveerimist

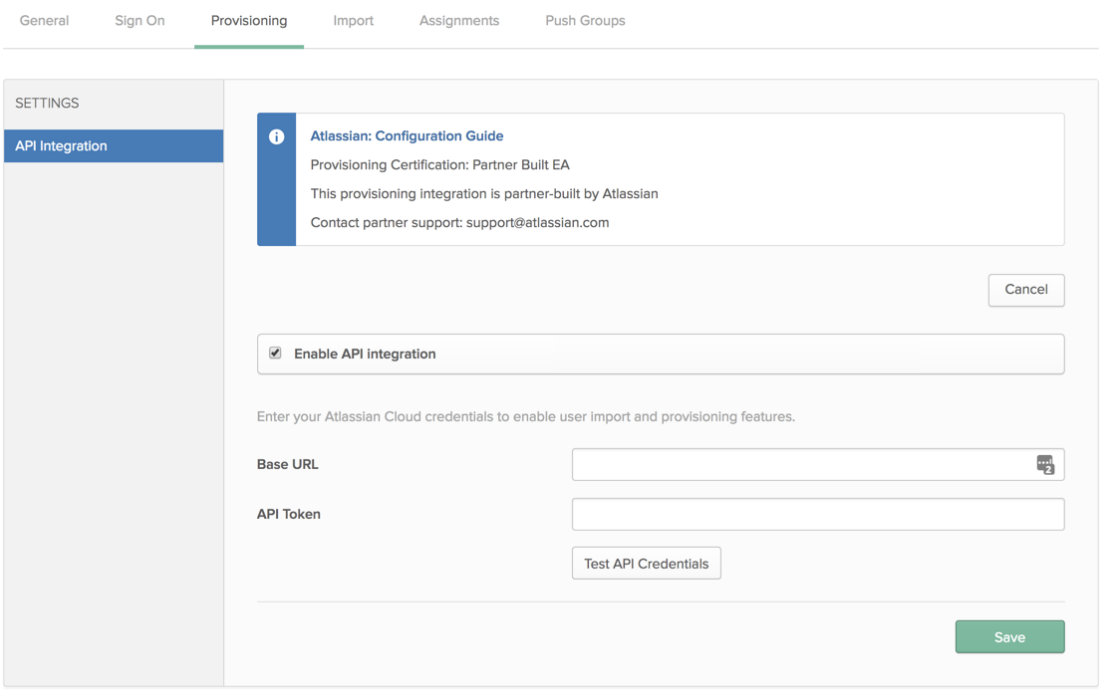
Järgneva sammuna tuli tegeleda duplikaatkontode probleemiga. Esialgne lootus oli, et Atlassian võimaldab ühele kasutajale kuuluvad erinevate domeenidega kontod ühendada, kuid see osutus võimatuks. Seetõttu tuli välja selgitada kumb kasutajakonto on kasutaja primaarne konto, selle ligipääs säilitada ning vajadusel see ka uuele domeenile üle liigutada. Enamus kasutajate puhul oli produktide ligipääsu järgi kerge välja selgitada primaarne kasutajakonto, kuid siiski tuli 42st kontost koosnev valim manuaalselt läbi töötada. Eelmainitud kontodest koostati uus CSV fail ning seejärel kasutati uuesti kasutajate deaktiveerimise skripti, vt. Lisa 2.

Duplikaatkontode sulgemise järel oli tarvis ka tagada, et kindlasti jääks vabaks bolt.eu aadress. Seda juhtudeks, kus kasutaja varasem primaarne konto oli taxify.eu domeeni peal kuid nüüd oli see vaja liigutada uue domeeni peale, mis aga on juba deaktiveeritud staatusesse liigutatud konto poolt kasutuses. Probleemi lahendamiseks lõin skripti, mis käib üle kõik suletud staatuses kontod, lisab emaili lõppu „-deactivated“ sõne, mis omakorda vabastab eesnimi.perenimi@bolt.eu formaadis emaili aadressi, vt. Lisa 3.

Järgnevalt liigutati kõik aktiivsed taxify domeenil olevad kasutajad bolt domeenile. Selle jaoks oli vaja eelmist skripti vaid minimaalselt muutma, vt. Lisa 4. Skripti abil liigutati uuele domeenile 23 kasutajat. Sellega loeti Atlassiani kasutajabaasi puhastamise faas lõpetatuks ning see võimaldas edasi liikuda automaatse provisioneerimise rakendamise etapiga.

6.3 Kasutajate automaatne provisioneerimine

Automaatse kasutajate provisioneerimise seadistamise esimeseks sammuks on Atlassian’i keskkonnas SCIM kataloogi loomine. Kataloogi luues väljastab Atlassian API võtme ja kataloogi aadressi, mida on hiljem Okta rakenduse seadistamisel tarvis (joonis 20).



Joonis 20. Atlassian Access provisioneerimise seadistamise vaade

Kui ühendus kahe portaali vahel on valideeritud, on võimalik määrata missuguste sündmuste puhul Okta rakendusega suhtleb. Sündmusteks võib olla kasutaja loomine, redigeerimine või deaktiveerimine. Samuti on võimalik kaardistada atribuudid, mis kasutajakontodele kirjutatakse, näiteks positsiooni nimetus või osakond, kus kasutaja parasjagu töötab.

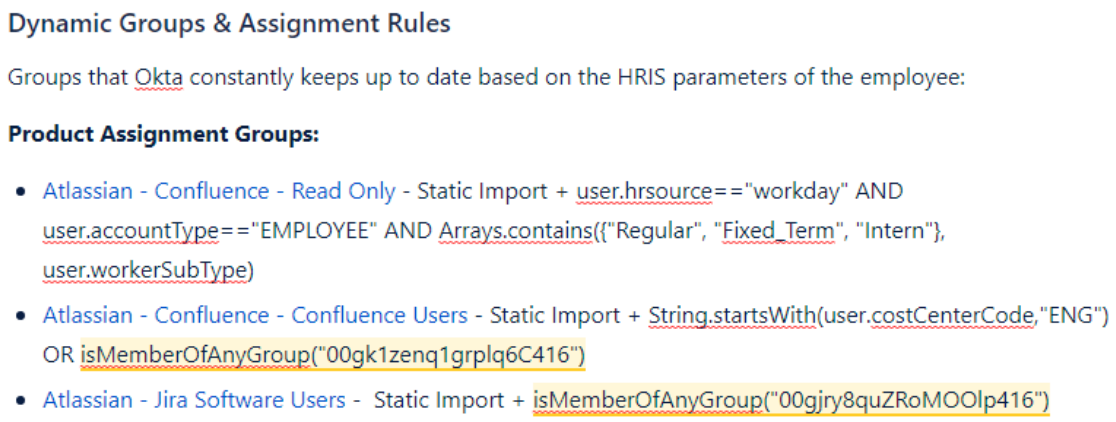
Kui Okta poolel on rakendus seadistatud, saab alustada kasutajagruppide loomisega. Kasutajagruppe kasutatakse Atlassian Cloud rakendusele ligipääsu andmiseks ning samuti on võimalik neid samu kasutajagruppe Atlassian'i keskkonda sünkroniseerida. Hiljem on võimalik Atlassian'i keskkonnas eelmainitud kasutajagruppe kasutada litsentside määramiseks ja ka iga Atlassiani toote tasemel ligipääsude haldamiseks, näiteks ühele konkreetsele Jira või Confluence projektile ligipääsu määramiseks.

Selleks, et tehtavate muutuste käigus vältida tõrkeid kasutajate töös, tuleb olemasolevad litsentse määravad grupid üks-ühele Atlassiani ja Okta vahel peegeldada. Kahjuks ei võimalda Okta kasutajaliides grupiliikmeskonda hulgi redigeerida, mistõttu tuli gruppide täitmise tarvis luua skript, mis seda läbi Okta API teha võimaldab, vt. Lisa 5.

Ülalmainitud skripti sisenditeks on CSV fail, mis on loodud Atlassiani kasutajagrupi liikmeskonna eksportimise tulemusena, ning vastava Okta grupi identifikaator kuhu

kasutajad soovitakse lisada. Iga kasutaja kohta tehakse *GET* päring Okta pihta ning küsitakse kasutaja emaili põhjal kasutajakonto unikaalset identifikaatorit [19]. Kui isikul on aktiivne konto olemas, lisatakse ta varasemalt *PUT* päringuga täpsustatud grupi liikmeks ning tulemused logitakse logifailidesse [20]. Vastavat skripti kasutades täideti kolm varasemalt manuaalselt hallatavat gruppi ning ka grupp, mille alla kõik aktiivsed Atlassian'i kasutajad kanda.

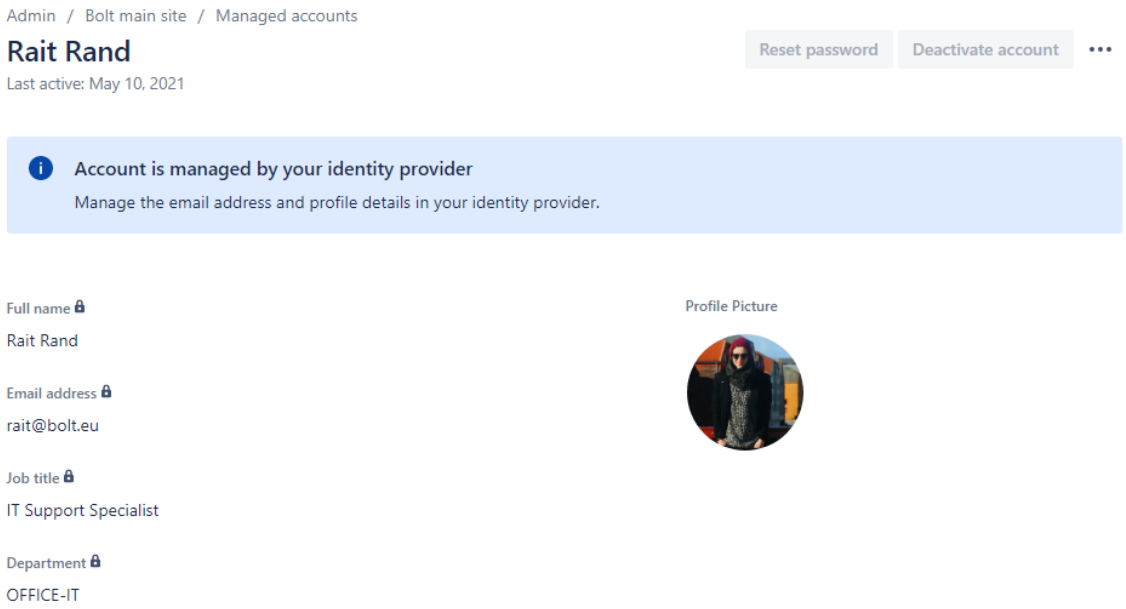
Praeguseks hetkeks on seega Okta'sse loodud staatiliselt täidetud, Atlassian'i gruppide liikmeskonda peegeldavad grupid, kuid nüüd oleks vaja nad hübriidgruppideks muuta. Hübriidgrupp on kasutajagrupp, kuhu on kasutajad määratud nii manuaalselt kui ka grupireegli põhjal. Grupireegleid on võimalik defineerida kõikide Okta profiilil olevate atribuutide kaudu, näited grupireeglitest leiab joonisel 21. Grupireegli olemasolu on hädavajalik, et uued ettevõttega liituvad töötajad automaatselt grupi liikmeteks lisada, kaotades ära vajaduse gruppe manuaalselt hallata.



Joonis 21. Grupireeglite näited

Kõiki eelmainitud gruppe kasutatakse Okta siseselt Atlassian Cloud rakendusele ligipääsu andmiseks. Rakenduse ligipääsu andmisega kaasneb kasutajaprofiili sünkroniseerimine Atlassian'i keskkonnas asuvasse SCIM kasutajakataloogi. Kui Okta poolt saadetud emailiaadressiga kasutaja on juba Atlassian'is olemas, muudetakse ta Okta poolt hallatava konto staatusesse, muuljuhul luuakse kasutajale uus Atlassiani konto. Juhul, kui kasutajakonto on muudetud Okta poolt hallatavaks, on kasutajaga seonduvaid muudatusi võimalik teha vaid Okta keskkonna kaudu ning administreerimine läbi Atlassian'i administraatorportaali pole enam võimalik. Näide Okta poolt hallatavast kasutajast on nähtav joonisel 22, millelt ilmneb, et profiiliatribuudid on lukus ning neid

pole võimalik muuta. Samuti ei ole võimalik uut parooli sätestada ega kontot deaktiveerida.

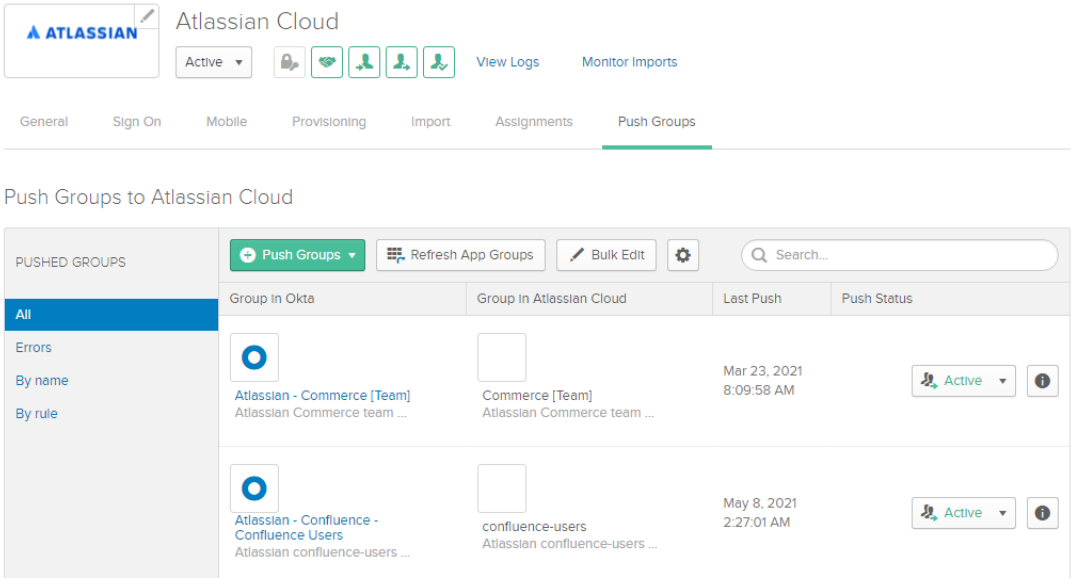


Joonis 22. Okta poolt manageeritud Atlassian'i profiil

Kuigi kasutajakontode provisioneerimine Atlassian keskkonda automatiseeriti, ei hõlma see automatsioon veel endas kasutajate litsentseerimist. Atlassian võimaldab automaatset produktide litsentseerimist läbi kasutajagruppide, mida käsitletakse järgnevas alapeatükis.

6.4 Atlassian gruppide sünkroonimine

Atlassian Cloud on üks väheseid rakendusi, mis toetab kasutajagruppide sünkroonimisfunktsiooni (joonisel 23). Sünkroonimine võimaldab Okta siseselt loodud kasutajagruppe sihtrakendusse sünkroonida selliselt, et neid pole tarvis enam käsitsi hallata. Automaatse sünkroonimise käigus uuendatakse Atlassian keskkonda loodud gruppide liikmeskonda automaatselt, identiteedihaldusteenuses defineeritud grupireeglite põhiselt. Seeläbi on sihtrakenduse siseselt võimalik gruppe kasutada kasutajaõiguste ja litsentside automaatseks haldamiseks [21]. Järgnevalt vaatleme kuidas on ettevõttes Bolt Technology OÜ kasutajagrupid koostatud ning neid litsentside ja ligipääsuõiguste jagamise automatiseerimiseks kastutatud.



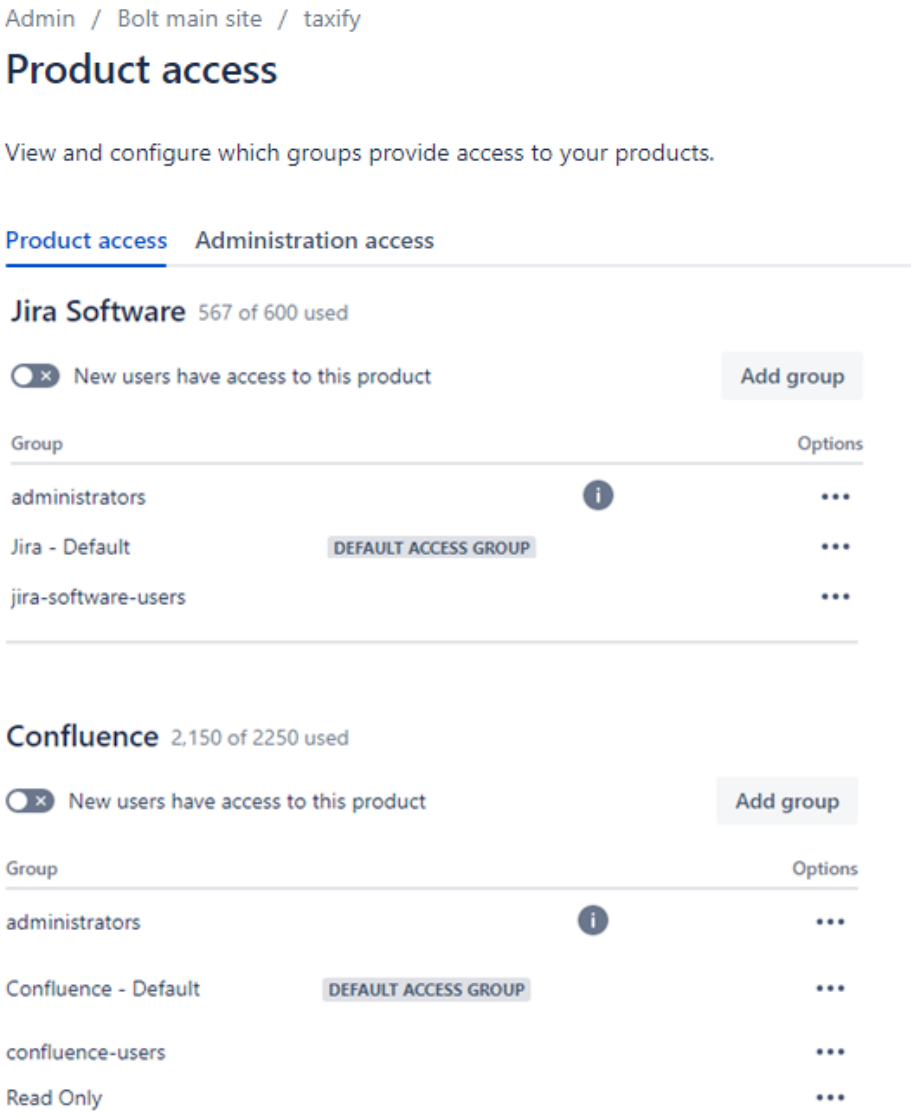
Joonis 23. Atlassian'i gruppide sünkroonimisfunktsioon

6.4.1 Toodetele ligipääsu võimaldavad grupid

Kuigi Atlassian ise soovitab Okta ja Atlassian'i gruppide sünkroniseerimisel alati uued grupid luua, otsustati nende soovituste vastu minna ning Okta pool loodud grupid olemasolevate Atlassian'i gruppidega liita. Soovitusi eirati vältimaks ulatuslikku manuaalset tööd Confluence projektide ja lehekülgedele ligipääsude taastamisel. Bolt'i Confluence peamine sait sisaldab endas kokku üle 600 projekti ning nende ligipääsude manuaalne läbivaatamine oleks olnud erakordselt tülikas ning aeganõudev ülesanne.

Automaatse litsentseerimise tarvis tuli esimese sammuna Atlassian'i keskkonnas iga produkti jaoks uus vaikimisi grupp luua. Vaikimisi gruppi lisatakse kasutajad, kellele on mingisuguse toote ligipääs määratud otse läbi Atlassian'i administraatorpaneeli. Uusi vaikimisi gruppe on tarvis, sest vastasel juhul kirjutaks Okta iga sünkroonimise käigus Atlassian'i keskkonnas asuva grupi andmed enda andmetega üle ning eemaldaks produkti ligipääsu kasutajatelt, kellele pole seda läbi Okta lubatud.

Uute vaikimisi gruppide (Jira – Default ja Confluence – Default) loomise järel lisati need Atlassiani produkti ligipääsude gruppide nimistusse (joonis 24). Sama nimistu alla lisati ka Okta hallatavad grupid (joonis 21). Järgnevalt sünkrooniti Oktas loodud grupid Atlassiani keskkonda ning ühendati selliselt, et Okta neid haldaks. Seega saavutati olukord, kus varasemalt IT meeskonna käes olnud Atlassian'i kasutajakontode manuaalne haldusprotsess on muudetud täisautomaatseks.



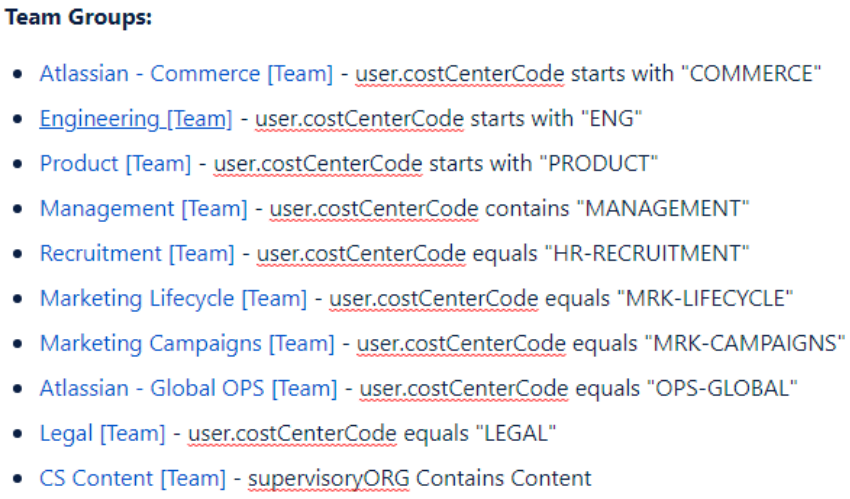
Joonis 24. Atlassian'i toodete ligipääsugrupid

6.4.2 Meeskonnapõhised grupid

Lisaks sellele, et Okta võimaldab IT meeskondadel oma protsesse automatiseerida võimaldab see ka lisaväärtust pakkuda ning seeläbi IT meeskonna teenuse kvaliteeti tõsta. Varasema protsessi raames ei olnud mõeldav, et IT tiim suudaks iga ettevõttes oleva meeskonna ning osakonna kohta eraldi kasutajagruppi manuaalselt hallata ning ajakohasena hoida, sest ettevõte struktuuris toimub pidevalt muutusi ning kasutajaid lisatakse ja kustutatakse igapäevaselt.

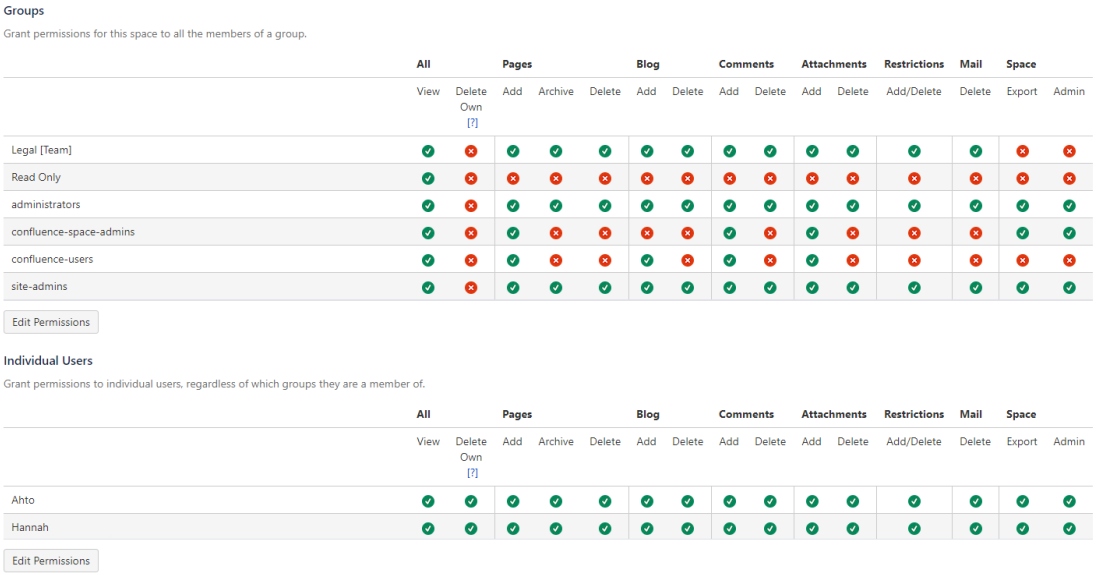
Mugavamaks haldamiseks võimaldab Okta luua meeskonna ja osakonna põhiseid gruppe, mida on samuti võimalik Atlassiani keskkonnaga sünkroniseerida. Gruppidesse jaotamine toimub Oktasse loodud reeglite põhjal mis on defineeritud *costCenterCode*

atribuute kasutades. Tänaseks on loodud järgnevad meeskonna- ja osakonnapõhised grupid (joonis 25). Vastavaid gruppe saab Atlassian'i produktide siseste ressursside ligipääsude haldamiseks kasutada. Näiteks privaatsete Confluence lehtede või meeskonnapõhiste Jira projektide ligipääsude automatiseerimiseks.



Joonis 25. Oktas loodud meeskonnagrupid ning nende reeglid

Järgnevalt vaatleme ühte konkreetset näidet õigusosakonna Confluence projektist, kuhu varasemalt oli kogu tiimile, ehk kaheksateistkümnele inimesele, ligipääsud individuaalselt jagatud. Okta võimaldas luua „Legal [Team]" nimelise grupi kuhu määratakse inimesi grupireegli põhjal (Joonis 26). Uus loogika kaotas ära vajaduse jagada ligipääse individuaalsel tasemel ning muuhulgas tagas, et grupiliikmeskond oleks dünaamiliselt muutuv. Seega kui mõni töötaja gruppi lisatakse või sealt eemaldatakse, toimuvad vastavad muutused ka töötaja Confluence ligipääsudes automaatselt. Näiteks uus õigusosakonna liige saaks grupireeglile vastamise korra ligipääsu automaatselt.



Groups

Grant permissions for this space to all the members of a group.

	All		Pages			Blog		Comments		Attachments		Restrictions	Mail	Space	
	View	Delete Own [?]	Add	Archive	Delete	Add	Delete	Add	Delete	Add	Delete	Add/Delete	Delete	Export	Admin
Legal [Team]	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Read Only	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
administrators	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
confluence-space-admins	✓	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✓
confluence-users	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗
site-admins	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Edit Permissions

Individual Users

Grant permissions to individual users, regardless of which groups they are a member of.

	All		Pages			Blog		Comments		Attachments		Restrictions	Mail	Space	
	View	Delete Own [?]	Add	Archive	Delete	Add	Delete	Add	Delete	Add	Delete	Add/Delete	Delete	Export	Admin
Ahto	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hannah	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Edit Permissions

Joonis 26. Confluence's kasutatav meeskonnagrupp

7 Kokkuvõte

Käesoleva diplomitöö eesmärgiks oli kaasajastada Bolt Technology OÜs kasutusel olnud kasutajakontode elutsüklihalduse värbamisprotsessi sammud. Seni kasutusel olnud protsessiga jätkamine oleks tähendanud, et kaasatud meeskonnad oleksid pidanud palkama juurde kümneid spetsialiste, et üha kasvava kompleksuse ning volüümidega toime tulla. Just seetõttu oli vaja värbamisprotsessi automatiseerida.

Töö käigus anti lugejale teoreetiline taust kasutaja digitaalsest identiteedist, identiteedi ja ligipääsude halduse valdkonnast üldiselt ning tööriistadest, mis halduse automatiseerimist võimaldasid. Järgnevalt visualiseeriti Bizagi Modeler tarkvara abil nii vana kui ka uue värbamisprotsessi kõik sammud ning kirjeldati kõikide protsessiga seotud meeskondade ülesandeid. Uue protsessi kirjelduse juures toodi välja ka kõik erinevad protsessiga seonduvad tegevused, mida Okta kohandatavad töövood automatiseerida võimaldasid. Edasi kajastati juba ühe tuumikrakenduse, Atlassian Cloud, liidestamist Oktaga, mis võimaldas automatiseerida kasutajakontode provisioneerimise, litsenseerimise ning sihtrakenduse siseste ligipääsuõiguste andmise. Liidestamise detailne kirjeldus andis ühtlasi aimu töö mahust mida oleks terve uue protsessi rakendamiseks tarvis teha.

Mahuliste piirangute tõttu keskenduti töös vaid värbamisega seonduva kasutajakonto haldusprotsessi etapile ning kirjeldati vaid ühe rakenduse liidestamise tarvis tehtud tööd. Antud töö edasiarenduse käigus oleks võimalik kaardistada ning automatiseerida ka kasutaja ettevõttes liikumise ja sellest lahkumisega seonduvad haldusportsessid. Lõplik töö kataks seega kasutajakonto elutsüklihalduse automatiseerimise tervikuna, värbamisest kuni ettevõttest lahkumiseni.

Kasutatud kirjandus

[1] „Free business process mapping and modeling software - Bizagi Modeler“. https://www.bizagi.com/en/platform/modeler (25.04.2021)

[2] „BPMN Specification - Business Process Model and Notation“. https://www.bpmn.org/ (25.04.2021)

[3] „What is Okta?“ https://support.okta.com/help/s/article/What-is-Okta?language=en_US (16.05.2021)

[4] „Okta Workflows | Okta“. https://www.okta.com/platform/workflows/ (16.05.2021)

[5] „About the lifecycle of a provisioned user | Okta“. https://help.okta.com/en/prod/Content/Topics/Provisioning/lcm/lcm-provisioning-workflow.htm (15.05.2021)

[6] „Definition of Identity and Access Management (IAM) - Gartner Information Technology Glossary“, *Gartner*. https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam (13.05.2021)

[7] „How Identity and Access Management Quietly Powers Your Company | Okta“. https://www.okta.com/identity-101/iam-powers-your-company/ (14.05.2021)

[8] „Digital Identity - an overview | ScienceDirect Topics“. https://www.sciencedirect.com/topics/computer-science/digital-identity (16.05.2021)

[9] „What is IDaaS? Understanding Identity as a Service | Okta“. https://www.okta.com/identity-101/idaas/ (14.05.2021)

[10] „Two-Factor Authentication vs. Multi-Factor Authentication | Okta Blog“. https://www.okta.com/blog/2016/12/two-factor-authentication-vs-multi-factor-authentication-what-are-the-risks/ (15.05.2021)

[11] „What is Single Sign-On (SSO) and How Does It Work? | Okta“. https://www.okta.com/blog/2021/02/single-sign-on-sso/ (15.05.2021)

[12] „Definition of Identity Management - Gartner Information Technology Glossary“, *Gartner*. https://www.gartner.com/en/information-technology/glossary/identity-management (14.05.2021)

[13] „Directory As a Service with Universal Directory | Okta“. https://www.okta.com/products/universal-directory/ (15.05.2021)

[14] „Okta User Migration Guide | Okta“. https://www.okta.com/resources/whitepaper/okta-user-migration-guide/ (15.05.2021)

[15] *ITIL Service Operation*. TSO (The Stationery Office), 2011.

[16] „Atlassian Access Pricing“. https://www.atlassian.com/software/access/pricing (10.05.2021)

[17] „Overview of Atlassian Access“, *Atlassian*. https://www.atlassian.com/software/access/guide/overview (10.05.2021)

[18] „The User management REST API REST API“. https://developer.atlassian.com/cloud/admin/user-management/rest/api-group-users/#api-users-account-id-manage-lifecycle-disable-post (10.05.2021)

[19] „Users | Okta Developer“. https://developer.okta.com/docs/reference/api/users/#get-user-with-login (17.05.2021)

[20] „Groups | Okta Developer“. https://developer.okta.com/docs/reference/api/groups/#add-user-to-group (17.05.2021)

[21] „Configure user provisioning with Okta“, *Atlassian Support*. https://support.atlassian.com/provisioning-users/docs/configure-user-provisioning-with-okta/ (17.05.2021)

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

Mina, Rait Rand

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Kasutajakonto elutsüklihalduse automatiseerimine Bolt Technology OÜ näitel" , mille juhendaja on "Siim Vene"
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

17.05.2021

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

Lisa 2 – Atlassian'i kasutajakontode deaktiveerimise skript

```
import csv
import requests
import json

url = "https://api.atlassian.com/users"
api = "manage/lifecycle/disable"
session = requests.Session()
response = session.get(url)

headers = {
    'Content-Type': "application/json",
    'Authorization': "Bearer <API KEY HERE>",
}

successRecord = open("disable-Success.csv", "w+")
successRecord.write("Name,Email,ID,Response\r")
failRecord = open("disable-Fail.csv", "w+")
failRecord.write("Name,Email,ID,Response\r")

with open('03.03 - Disable Taxify Trello users.csv') as csv_file:
    csv_reader = csv.reader(csv_file, delimiter=',')
    line_count = 0
    #Skip the header row
    next(csv_reader)
    for row in csv_reader:
        userName = str(row[0])
        userEmail = str(row[1])
        id = str(row[2])

        payload = json.dumps( {
            "message": "This account has been using the old Taxify email
domain and has been scheduled for deletion"
        } )

        app_endpoint = url + "/" + id + "/" + api
        response = requests.request(
            "POST",
            app_endpoint,
            data=payload,
            headers=headers
        )

        #check for 204 token_response
        if response.status_code == 204:
            print("User " + userEmail + " processed OK")
            successOutput = (userName + "," + userEmail + "," + id + "," +
response.text + "\r")
            successRecord.write(successOutput)
```

```
            line_count += 1
        else:
            print("something happened here with user " +
                  userEmail)
            failedOutput = (userName + "," + userEmail + "," + id + "," +
response.text + "\r")
            failRecord.write(failedOutput)
    print(response.text)
    print(f'Processed {line_count} lines.')
    successRecord.close()
    failRecord.close()
```

Lisa 3 – Astlassian kasutajakontode emaili muutmise skript

```
import csv
import requests
import json

url = "https://api.atlassian.com/users"
api = "manage/email"
session = requests.Session()

response = session.get(url)
headers = {
    'Content-Type': "application/json",
    'Authorization': "Bearer <API KEY HERE>",
}

with open('Deactivated users.csv') as csv_file:
    csv_reader = csv.reader(csv_file, delimiter=',')
    line_count = 0
    #Skip the header row
    next(csv_reader)
    for row in csv_reader:
        userName = str(row[0])
        userEmail = str(row[1])
        id = str(row[2])

        #Deactivated user email format
        splitEmail = userEmail.split("@")
        newEmail = splitEmail[0] + "-deactivated@" + splitEmail[1]

        payload = json.dumps( {
            "email": newEmail
        } )

        app_endpoint = url + "/" + id + "/" + api
        response = requests.request(
            "PUT",
            app_endpoint,
            data=payload,
            headers=headers
        )
```

Lisa 4 – Atlassian kasutajakonto emaili domeeni muutmise skript

```
import csv
import requests
import json

url = "https://api.atlassian.com/users"
api = "manage/email"
domain = "bolt.eu"
session = requests.Session()

response = session.get(url)
headers = {
    'Content-Type': "application/json",
    'Authorization': "Bearer <API KEY HERE>",
}

with open('Active Taxify users.csv') as csv_file:
    csv_reader = csv.reader(csv_file, delimiter=',')
    line_count = 0
    #Skip the header row
    next(csv_reader)
    for row in csv_reader:
        userName = str(row[0])
        userEmail = str(row[1])
        id = str(row[2])

        # Email format for migrating users from Taxify -> Bolt
        newEmail = userEmail.split("@")[0]+ "@" + domain

        payload = json.dumps( {
            "email": newEmail
        } )

        app_endpoint = url + "/" + id + "/" + api
        response = requests.request(
            "PUT",
            app_endpoint,
            data=payload,
            headers=headers
        )
```

Lisa 5 – Okta gruppide täitmise skript

```
import csv
import requests

url = "https://bolt.okta.com/api/v1/groups"
api = "/{groupId}/users/{userId}"
session = requests.Session()

#Headers
response = session.get(url)
payload  = {}
headers = {
    'Content-Type': "application/json",
    'Authorization': "SSWS <API KEY HERE>",
}

oktaGroup = input ("Enter the Okta group ID: ")
csvFileName = input("Enter the CSV file name without the extention: ")

#Logging files
successRecord = open(csvFileName + "-Success.csv", "w+")
successRecord.write("Username,ID\r")
failRecord = open(csvFileName + "-Fail.csv", "w+")
failRecord.write("Username,ID\r")

with open(csvFileName + ".csv") as csv_file:
    csv_reader = csv.reader(csv_file, delimiter=',')
    line_count = 0
    next(csv_reader)
    for row in csv_reader:
        userEmail = str(row[0]).split("@")

        # Read email from CSV and Get Okta userID
        responseUser = requests.get(

"https://bolt.okta.com/api/v1/users/{username}%40{domain}".format(username=us
erEmail[0], domain=userEmail[1]),
            data=payload,
            headers=headers)

        #Check if Atlassian user can be found using email (HTTP 200)
        if responseUser.status_code == 200:
            responseUser = responseUser.json()
            id = responseUser["id"]

            # Adding a user to a specific group in Okta and logging the
action based on response code
            app_endpoint = url + api.format(groupId=oktaGroup, userId=id)
```

```
            response = requests.request("PUT", app_endpoint, data=payload,
headers=headers)

            # Check if group addition successful (HTTP 204)
            if response.status_code == 204:
                print("User " + userEmail[0] + " processed OK")
                successOutput = (id + "," + userEmail[0] + "\r")
                successRecord.write(successOutput)
                line_count += 1
            else:
                print("Something happened here when adding the user " +
userEmail[0] + " to Okta group")
                failedOutput = (id + "," + userEmail[0] + "\r")
                failRecord.write(failedOutput)
        else:
            print("User does not have an account on Okta with the username: "
+ userEmail[0])
            failedOutput = (id + "," + userEmail[0] + "\r")
            failRecord.write(failedOutput)

    print(f'Processed {line_count} lines.')
    successRecord.close()
    failRecord.close()
```