

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kaspar Bankier 184987IADB

AS-i SEB Pank pääsuõiguste süsteemide inventeerimine

Bakalaureusetöö

Juhendaja: Meelis Antoi
Magistrikraad

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: Kaspar Bankier

17.05.2021

Annotatsioon

Käesoleva bakalaureusetöö eesmärgiks on luua ettevõttele AS SEB Pank lahendus pääsuõiguste süsteemide inventeerimiseks, mis vastab ettevõtte poolsetele nõuetele. Analüüsi käigus leitakse, kui vajalik on pääsuõiguste inventeerimise ning võimalikest ohtudest, kui seda ei tehta. Kirjeldatud on ka töös kasutatavad tehnoloogiad ning arhitektuur ja on antud ülevaade lõplikust lahendusest, koos töö käiguga.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 27 leheküljel, 6 peatükki, 19 joonist.

Abstract

Recertification of access right systems in AS SEB Pank

The aim of this bachelor's thesis is to create a solution for AS SEB Pank for recertifying access rights systems that meets the requirements of the company. The analysis will identify the need for recertifying access rights and the potential risks of not doing so. The technologies and architecture used in the work are also described and an overview of the final solution is given, together with the course of the work.

The thesis is in Estonian and contains 27 pages of text, 6 chapters, 19 figures.

Lühendite ja mõistete sõnastik

AJAX	<i>Asynchronous JavaScript And XML</i> , tehnikad interaktiivsete veebirakenduste loomiseks
API	<i>Application Programming Interface</i> , rakendusliides
<i>Development</i> keskkond	Arenduskeskkond, millele pääseb ligi arendusmeeskond
DTO	<i>Data Transfer Object</i> , objekt mis kannab andmeid protsesside vahel
<i>echo</i>	PHP avaldis teksti kuvamiseks
Inventeerimine	Protsess, mille käigus kontrollitakse, mis töötajatele mis pääsuõigused määratud on.
<i>Live</i> keskkond	Keskkond, millele pääseb ligi iga ettevõtte töötaja
Objekt	Abstraktne andmetüüp
ORM	<i>Object Relational Mapper</i>
PDF	<i>Portable Document Format</i> , dokumentide vorming
PHP	<i>PHP: Hypertext Preprocessor</i>
POST	Päringu tüüp, millega edastatakse serverile andmeid
Primaarne omanik	Pääsuõiguse või süsteemi eest peamine vastutav isik
Pääsuõigus	Luba mingi tegevuse sooritamiseks, seda näiteks mingis rakenduses
SQL	<i>Structured Query Language</i> , andmebaasides kasutatav programmeerimiskeel
Süsteem	Kogum sarnastest pääsuõigustest, näiteks kõik pääsuõigused mingi teatud rakenduse kasutamiseks.
<i>Test</i> keskkond	Testkeskkond, millele pääseb ligi arendusmeeskond ning administratiivne pool
XLSX	Excel-i tabelite vorming

Sisukord

Sissejuhatus	9
1 Ülevaade	10
1.1 AS SEB Pank.....	10
1.2 Ettevõtte turvapoliitika	10
1.2.1 Kasutajaõiguste register.....	11
1.3 Töökorraldus.....	11
1.3.1 Agiilne arendus.....	11
1.3.2 Versioonihaldus.....	13
1.4 Eelnevalt loodud lahendus.....	13
1.4.1 Inventuuride loomine ning haldamine.....	13
1.4.2 Inventuuride haldamine.....	13
1.4.3 Inventuur juhile	14
2 Probleem.....	15
2.1 Aktuaalsus	15
2.2 Nõuded.....	16
3 Lahendus.....	17
3.1 Arhitektuur.....	17
3.1.1 Esitlustasand	17
3.1.2 Rakenduse tasand	17
3.1.3 Andmetasand	17
3.1.4 Võrdlus	17
3.2 Kasutatavad tehnoloogiad.....	18
3.2.1 Twig.....	18
3.2.2 Slim.....	18
3.2.3 Doctrine	19
3.2.4 Phinx.....	19
3.2.5 BIRT	19
3.2.6 cron	19
3.2.7 jQuery	19

3.3 Teostus.....	20
3.3.1 Primaarsete omanike määramine.....	20
3.3.2 Aken pääsuõiguste süsteemi inventuuri loomiseks	20
3.3.3 Vaade inventuuris osalevale töötajale	21
3.3.4 Taotluste loomine	23
3.3.5 Teavitused.....	23
3.3.6 Vaade inventuuri haldamiseks.....	23
3.3.7 Raportid	24
3.3.8 Konsool.....	25
3.4 Koodinäited	26
3.4.1 Interaktiivsus	26
3.4.2 Kontrollerid	28
3.4.3 Twig-i mallid.....	29
3.4.4 Teenused.....	30
3.4.5 <i>Mapper</i> ja DTO	31
3.4.6 Repositooriumid	31
3.4.7 Raportid	32
3.5 Testimine	32
3.6 Probleemid.....	33
4 Tulemused	34
4.1 Hinnang	34
4.2 Tagasiside	34
4.3 Tuleviku arendused.....	34
Kokkuvõte	35
Kasutatud kirjandus	36
Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks	38
Lisa 2 – Osa genereeritud XML-failist raporti loomiseks	39

Jooniste loetelu

Joonis 1. Jira keskkonnas olev ülesanne.....	12
Joonis 2. Näide petumeilist.....	15
Joonis 3. Kolmetasandiline arhitektuur	17
Joonis 4. Kujutletav näide DBAL-i ja ORM-i kasutamisest – raamatute väljastamine andmebaasist.....	19
Joonis 5. Primaarse omaniku määramine	20
Joonis 6. Süsteemi inventuuri loomise aken.....	21
Joonis 7. Inventuuri vaade töötajale	22
Joonis 8. Pääsuõiguse täpsem ülevaade.....	22
Joonis 9. Taotluste kogum (ühe taotlusega)	23
Joonis 10. Inventuuri haldamise vaade.....	24
Joonis 11. Raport PDF vormingus.....	25
Joonis 12. Raport XLSX vormingus	25
Joonis 13. Inventuuride käskluse käivitamine konsooli kaudu	26
Joonis 14. Inventuuri valideerimine ning kinnitamine	27
Joonis 15. Pääsuõiguse primaarse omaniku muutmise päringuga tegelemine router-is.	28
Joonis 16. Kontrolleri funktsioon inventuuri haldusvaate kuvamiseks	29
Joonis 17. Pääsuõigustega seotud rollide kuvamise Twig-i mall	30
Joonis 18. Teenuse funktsioon süsteemi inventuuri loomiseks.....	31
Joonis 19. Kriteeriumitele vastavate inventuuride andmebaasist väljastamine kasutades QueryBuilder-it.....	32

Sissejuhatus

Tänapäevastes ettevõttes on infoturve tähtsal kohal, kahju võimalikust küberrünnakust võib olla äärmiselt suur. Selleks on infoturbe jaoks välja töötatud paljusid meetmeid, ühe sellise meetme loomine on käesoleva bakalaureusetöö eesmärgiks, nimelt luua ettevõttes AS SEB Pank kasutatavale kasutajaõiguste registrile lahendus pääsuõiguste süsteemide inventeerimiseks.

Pääsuõiguste süsteemide inventeerimine on ettevõtte poolt kirjeldatud protsess, mille käigus pääsuõiguste omanikud kontrollivad, millistel töötajatel antud pääsuõigus on määratud ning kas töötajate tööülesannetest lähtuvalt see kas alles jätta või eemaldada. Inventuure hakkavad läbi viima kasutajaõiguste registri administreerimise eest vastutavad isikud.

Käesolev bakalaureusetöö analüüsib ka pääsuõiguste haldamise vajadust ning toob välja võimalikud ohud, mida kehv pääsuõiguste haldamine kaasa võib kaasa tuua.

Loodav lahendus kindlustab selle, et töötajatel oleksid määratud ainult need pääsuõigused, mis on neile tööks vajalikud. Arenduse käigus pannakse ka rõhku sellele, et loodav lahendus oleks võimalikult intuitiivne nii kasutajaõiguste registri administratiivse poole jaoks kui ka töötajate jaoks, kes oma valduses olevaid pääsuõigusi üle vaatama peavad.

1 Ülevaade

1.1 AS SEB Pank

AS SEB Pank on Eestis tegutsev pank.

SEB põhiväärtused on kliendikesksus, pühendumus, koostöö ja lihtsus.

- Kliendikesksus – kliendi vajadused on seatud esikohale, püüdes alati pakkuda tõelist väärtust.
- Pühendumus – klientidel aidatakse saavutada edu ja vastutatakse enda tegevuste eest.
- Koostöö – ühtse meeskonnana töötades saavutatakse rohkem.
- Lihtsus – püüdelakse lihtsuse poole kõiges, mis keeruline.

Ettevõtte püüdleb selle poole, et need väärtused kajastuksid kõikides nende igapäevastes tegevustes, seal hulgas suhtluses klientide, kolleegide ja teiste osapooltega [1].

Käesoleva bakalaureusetöö kirjutamise hetkeks on autor töötanud ettevõttes ligikaudu ühe aasta.

1.2 Ettevõtte turvapoliitika

Kuna tegemist on suure pangandusvaldkonda kuuluva ettevõttega, peab infovarade turvalisus olema väga tähtsal kohal – nimelt on pangandusvaldkonda kuuluvad ettevõtted ühed peamised küberrünnakute ohvriteks langevatest ettevõtetest [2]. Selleks on kõik ettevõtte infovarad turvatud pääsuõigustega. Ettevõttes käib kõik pääsuõigustega seonduv läbi kasutajaõiguste registri.

1.2.1 Kasutajaõiguste register

Kasutajaõiguste registri kaudu on võimalik töötajal endale (või töötaja juhil töötajale) pääsuõigusi taotleda. Reeglina käib pääsuõiguste omandamine vaid läbi taotluste – nii jääb märk maha sellest, kes mingit pääsuõigust omab (või on omanud). Taotlemise protsess on järgnev:

1. Töötaja või töötaja juht esitab taotluse mingi pääsuõiguse omandamiseks.
2. Juht kinnitab taotluse (kui taotlejaks on töötaja).
3. Olenevalt pääsuõigusest kinnitab taotluse ka pääsuõiguse omanik.
4. Pääsuõigus määratakse töötajale.

Kasutajaõiguste registris on grupeeritud pääsuõigused haldamise huvides süsteemidesse, mis lihtsustavad ka pääsuõiguste taotlemist, vajaliku pääsuõiguse leidmiseks peab teadma vaid süsteemi nime.

Kasutajaõiguste registri kaudu on võimalik taotleda ka rolle (rollid sisaldavad endas pääsuõigusi mingi ametikoha jaoks), kuid käesolevas bakalaureusetöös käsitletakse peamiselt pääsuõigustega seotud teemasid.

1.3 Töökorraldus

1.3.1 Agiilne arendus

Töö arendusmeeskonnas toimub agiilse arenduse kohaselt *sprint*-ides, mis kujutavad endast lühikest ajaraami, mille sees tehakse ära eelnevalt planeeritud ülesanded [3]. Arendusmeeskonnale ülesannete andmine on tooteomaniku kohustus, kes on kasutajaõiguste registri eestkostja. Arendusmeeskonnas on ühe *sprint*-i pikkuseks kaks nädalat.

Sprint-i algab *planning* koosolekuga, mille raames jagatakse arendusmeeskonna seas ära ülesannete nimekirjast (ehk *backlog*-ist) võetud ülesanded, mis peaksid *sprint*-i jooksul valmis saama [4]. Ülesannete haldamiseks kasutatakse Jira tarkvara, iga ülesande juurde märgitakse ära selle lahendamiseks kulunud aeg (Joonis 1).

Identity and Access right Management / IAM-103
KEEP and REMOVE buttons

Edit Comment Assign More

Email Export

Details

Type: Improvement Status: **CLOSED**
 Priority: Minor (View Workflow)
 Resolution: Implemented

Labels: None
 System: RIILUL
 Business project: Line
 TU link: <https://jira.lpb.baltic.seb.net/browse/TU-24722>
 Epic Link: **IAM Epic for: Recertification of access roles and systems**
 Story Points: 4
 Sprint: Riil Sprint 10
 Releasable: With testcase
 Tips For Testing: Code ready.

Description

Keep and Remove buttons change status in revision_approval_item table. After pressing either button, X appears with text that says either KEEPING or REMOVING.

Pressing X resets the status (not reviewed -> 1).

Pressing button also does additional checks - if the revision is active or closed, if the approver is the logged in employee who can approve this row. Please view additional checks from Manager approval KEEP/REMOVE logic.

Time Tracking

Estimated: Not Specified
 Remaining: 0h
 Logged: 7.25h
 Include sub-tasks

Development

Agile

Joonis 1. Jira keskkonnas olev ülesanne

Sprint-i keskpaigas toimub (*backlog refinement*) koosolek, mille raames jagatakse uued ülesanded väiksemateks ülesanneteks ning kirjeldatakse need põhjalikult lahti, samuti käiakse üle *backlog* ja seatakse seal ülesanded tähtsuse järjekorda [5]. Nende koosolekute raames kirjeldatakse ülesanded ette ligikaudu kaheks järgneva*s sprint*-iks.

Sprint lõppeb *retrospective* koosolekuga, mille raames arutatakse, mis läks eelmisel *sprint*-il hästi või halvasti. Tekkinud probleemidele proovitakse koheselt leida lahendus.

Lisaks toimub iga tööpäev alguses lühike koosolek (*stand-up*), mille raames räägitakse, kuidas töö eelmisel päeval läks, mis probleemid tekkisid ja mida plaanitakse teha täna [4].

Võrreldes agiilset metoodikat klassikalise koskmudeliga, on agiilsel arendusel mitmeid eeliseid:

- Projektis on lihtne muudatusi teha – ülesannete prioriteet on alati muudetav, lõplik visioon projektist ei pea selge olema [6].
- Projekt valmib osadena – igat valminud osa saab juba testima hakata, seega vigade tuvastamine on kiirem, kui testida projekti kui tervikut [6].

- Pidev kommunikatsioon – läbi tihedate koosolekutega saab probleemseid olukordi kohe lahendada asuda [6].

1.3.2 Versioonihaldus

Arendusmeeskonnas kasutatakse versioonihalduseks Bitbucket platvormi. Bitbucket-i kasutamine annab võimaluse kõikide koodimuudatustega järge pidada ja võimaldab mugavalt koodi ülevaatusi sooritada – iga muudetud failirea kohta on arendusmeeskonna liikmetel võimalik kommentaare teha.

1.4 Eelnevalt loodud lahendus

Eelnevalt on loodud lahendus mis võimaldab juhtidel kontrollida oma töötajatele määratud pääsuõigusi ning rolle. Sellele põhinedes loob autor lahenduse pääsuõiguste süsteemide inventeerimiseks.

1.4.1 Inventuuride loomine ning haldamine

Inventuuri loomisel on vajalikud järgnevad andmed:

- Periood – inventuuri algus- ning lõpukuupäev.
- Meeldetuletuste tihedus – kui tihti (mitme päeva tagant) teavitatakse juhte, et käimas on inventuur ning neil on vaja oma töötajad üle kontrollida.
- Tihedus – mis aja tagant (päevades) inventuur uuesti käivitatakse.
- Riik – mis riigi juhid inventuuri kaasatakse, vaikimisi kõik Baltimaad, kuid võib valida ka üksiku riigi (Eesti, Läti, või Leedu).
- Kontakt email – inventuuri eest vastutava isiku email.

Kui kätte jõuab inventuuri alguskuupäev, siis käivitab inventuuri automaatne protsess, samuti sulgeb automaatne protsess inventuuri, kui kätte jõuab selle lõpukuupäev.

1.4.2 Inventuuride haldamine

Inventuuride haldusvaates saab inventeeritavaid töötajaid kellelegi teisele inventeerimiseks määrata (kui töötaja eest vastutav juht on näiteks pikemaks ajaks eemal) või töötajaid inventuurist üldse välja arvata (kui töötaja on näiteks ettevõttest lahkunud).

Iga juhi kohta on võimalik koostada raport, mis sisaldab endas informatsiooni juhi alluvuses olevate töötajate ning töötajate kõikide pääsuõiguste ning rollide ülevaatusena kohta.

1.4.3 Inventuur juhile

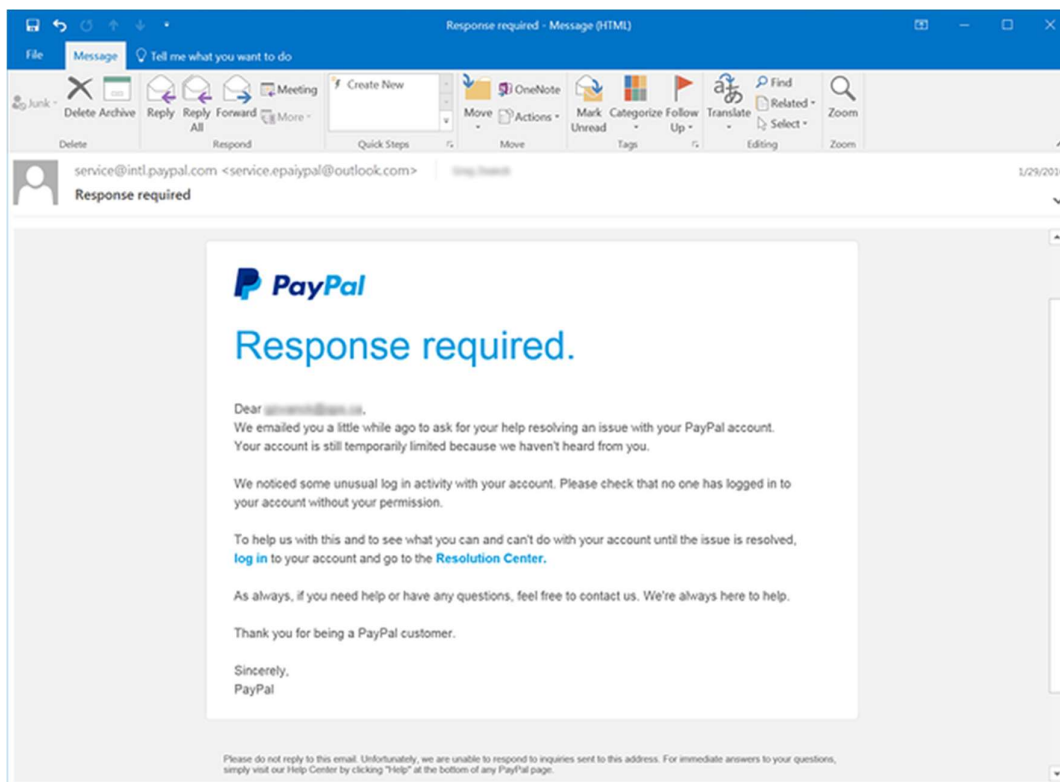
Iga töötaja all on näha temale määratud pääsuõigused ning rollid, mida saab kas eemaldamiseks või alles jätmiseks märkida. Kui kõik pääsuõigused ning rollid on üle vaadatud, siis peab andma lõpliku kinnituse. Peale seda enam muudatusi teha ei saa ning kõik eelnevalt valitud eemaldamised jõustuvad.

2 Probleem

2.1 Aktuaalsus

Ettevõtetes on tihti peale töötajatel ligipääsu andmetele, mida nad näha ei tohiks. Ponemon Institute-i poolt korraldatud uuringus, mis kaasas endas Saksamaa, Prantsusmaa, Suurbritannia ning Ameerika Ühendriikide ettevõtteid, selgus, et tervelt 71% lõppkasutajatest väidavad, et on omanud ligipääsu andmetele, mida nad näha ei tohiks. Nendest omakorda 54% väidavad, et ligipääs on olnud sagedane [7].

Infovarade turbe kõige nõrgem lüli on inimene – ning küberrünnakud on tänapäeval ainult kasvav probleem. Küberkurjategijal võib olla väga lihtne petta töötajalt välja näiteks kuhugi sisselogimiseks tarvis olevaid andmeid, seda enam, kui töötajal puudub IT-alane vilumus – kui andmeid proovitakse välja petta näiteks meiliteel, siis küberkurjategijate poolt saadetud meilid võivad olla vägagi usutavad (Joonis 2) [8].



Joonis 2. Näide petumeilist

Arvestades seda riski võib väita, et töötajate pääsuõiguste kontrollimine on oluline – tagajärjed võivad olla suured.

Töötajate pääsuõigusi kontrollivad nende vastavad juhid juba praegugi, kuid sellest jääb väheks. Ettevõttes on erinevaid pääsuõigusi üle saja tuhande ning juht ei pruugi teada, mida mõni pääsuõigus üldse võimaldab (seda kinnitab ka vestlus kasutajaõiguste registri administratiivse poolega) – liigagi lihtne on sellises olukorras antud pääsuõigus lihtsalt igaks juhuks alles jätta. Loodav lahendus leevendab seda probleemi, sest pääsuõiguste vastutavatel isikutel on paremad teadmised sellest, mida nende hallatavad pääsuõigused teevad.

2.2 Nõuded

Ettevõtte nõuded näevad ette, et teatud aja tagant peab kontrollima, mis töötajatele mis pääsuõigused antud on ning kas töötaja praegustest tööülesannetest lähtuvalt need kas alles jätta või eemaldada.

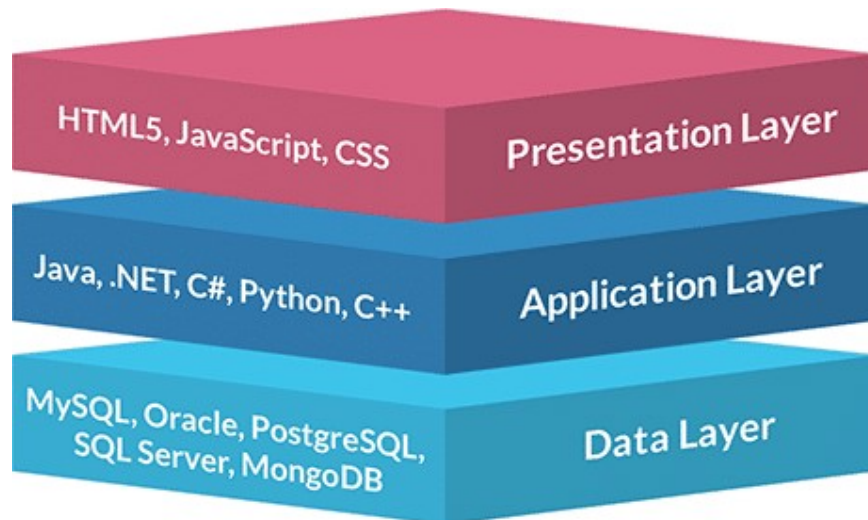
Nõuete täitmisega on ettevõttes juba algust tehtud, eelnevalt loodud juhtidele mõeldud inventuuri näol.

Loodav lahendus peab võimaldama pääsuõiguste eest vastutavatel isikutel kontrollida, millistele töötajatele tema valduses olevad pääsuõigused määratud on ning samamoodi kas need eemaldamiseks märkida või alles jätta – seega pääsuõiguste kontroll on kahepoolne.

3 Lahendus

3.1 Arhitektuur

Kasutajaõiguste register järgib kolmetasandilist arhitektuuri. Kolm tasandit jagunevad esitlustasandiks, rakenduse tasandiks ning andmetasandiks (Joonis 3) [9].



Joonis 3. Kolmetasandiline arhitektuur

3.1.1 Esitlustasand

Esitlustasand koosneb kasutajaliidesest. See kasutajaliides on sageli graafiline, millele pääseb juurde veebibrauseri või veebipõhise rakenduse kaudu ja mis kuvab lõppkasutajale sisu ja teavet [9].

3.1.2 Rakenduse tasand

Rakendustasand sisaldab funktsionaalset äriloogikat, mis juhib rakenduse põhivõimalusi [9].

3.1.3 Andmetasand

Andmetasand koosneb andmebaasist ja andmetele juurdepääsu kihist [9].

3.1.4 Võrdlus

Kolmetasandilist arhitektuuri saab võrrelda kahetasandilise arhitektuuriga – erinevuseks on see, et kahetasandilise puhul on esitlustasand ja rakenduse tasand ühes. Kahetasandilist

arhitektuuri kasutavad rakendused on enamasti väiksema keerukusega kuid võivad olla lõppkasutaja jaoks halvema jõudlusega, kuna siis tehakse rohkem tööd kasutaja seadmes [10]. Arvestades kasutajaõiguste mahukat ärioloogikat, hindab autor, et kolmetasandiline arhitektuur on kasutajaõiguste registri jaoks parim valik.

3.2 Kasutatavad tehnoloogiad

Kasutajaõiguste registri tagarakend on kirjutatud PHP-s (*PHP: Hypertext Preprocessor*). PHP on üldotstarbeline skriptimiskeel, mis sobib eriti veebiarenduse jaoks [11]. Kuigi PHP ei ole kõige populaarsemate programmeerimiskeelte seas (2020. aastal Stack Overflow poolt korraldatud küsitluse järgi on PHP programmeerimiskeelte edetabelis 20. kohal [12]), siis leiab see siiski tänapäeval laialdast kasutust – hetkel kasutab PHP-d tervelt 79.2% veebisaitidest [13]. Käesoleval aastal tuli välja ka PHP suur uuendus, PHP 8.0 [11], seega keele arendamisega tegeletakse veel aktiivselt.

Autoril on programmeerimiskeeltest PHP-ga kõige rohkem kogemust ja loodava lahenduse juures mängib kõige suuremat rolli just tagarakend, seega on lahenduse loomine mõneti lihtsam, kui mõne teise programmeerimiskeelega.

3.2.1 Twig

Kasutajaõiguste registris kasutatakse andmete kuvamisel Twig mallimootorit. Mallimootori kasutamine teeb andmete kuvamise mugavaks, andmete kättesaamine andmebaasist ning nende kuvamine on täiesti lahus, seega on kirjutatav kood loetavam. Mallides saab kasutada ka Twig-i enda süntaksit, mis võimaldab näiteks tsükleid ning tingimuslauseid luua [14].

3.2.2 Slim

Slim on väike PHP raamistik, millega saab luua veebirakendusi ning API-si (*Application Programming Interface*) [15]. Kasutajaõiguste registri uuemad arendused järgivad kolmetasandilist arhitektuuri, mida Slim-ile tuginedes teostatakse, sellega luuakse esitlustasandi kontrollereid. Samuti on loodud Slim-i abil API, mille kaudu uuemad arendused päringuid teevad. Slim sobib hästi väiksema veebirakenduse jaoks, kus suuremahulise raamistiku kasutamine ei ole vajalik [16].

3.2.3 Doctrine

Doctrine on kogum erinevatest tekidest, mille peamiseks rõhuks on ORM (*Object Relational Mapper*) ja DBAL (*Database Abstraction Layer*) [17]. Doctrine-i DBAL võimaldab andmebaasiga suhtlemist läbi PHP, ORM võimaldab andmebaasist saadud kirjade kohesest kasutamist PHP objektidena (Joonis 4).

```
$qb = $this->getEntityManager()->createQueryBuilder()
->select('b')
->from(Book::class, 'b');
$books = $qb->getQuery()->getResult();
$bookName = $books[0]->getName();
```

Joonis 4. Kujutatav näide DBAL-i ja ORM-i kasutamisest – raamatute väljastamine andmebaasist
See tähendab, et puudub vajadus kirjutada traditsioonilisi (ja andmebaasist sõltuvaid) SQL-lauseid (*Structured Query Language*) ning andmebaasist saadud kirjetest ei pea käsitsi objekte tegema – seega on kirjutatav kood lühem ja kergemini hallatav [18].

3.2.4 Phinx

Phinx-i kasutatakse andmebaasi migratsioonide (ehk andmebaasi struktuuri muudatuste) haldamiseks. Migratsioone saab kirjutada PHP keeles ning need ei sõltu kasutatavast andmebaasist [19].

3.2.5 BIRT

BIRT on Java-l põhinev tarkvara, mida kasutatakse andmete visualiseerimise ja aruannete loomiseks, mida saab kasutada veebirakendustes [20].

3.2.6 cron

cron on Unix-i laadsete operatsioonisüsteemide tööriist ajastatult ning automaatselt käskluste käivitamiseks [21].

3.2.7 jQuery

jQuery on funktsiooniderikas JavaScripti teek. See muudab HTML-dokumentide manipuleerimise, sündmuste käitlemise ja AJAX-i (*Asynchronous JavaScript And XML*) tehnikate rakendamise lihtsamaks [22].

3.3 Teostus

Teostusel on autor võtnud eesmärgiks järjepidevuse – luua lahendus võimalikult sarnane olemasolevale juhi inventuuri lahendusele. Nii on kasutajaõiguste registri administratiivsel poolele inventuuride loomine ja haldamine juba tuttav, seda ka neile kes inventuure sooritama peavad. Lisaks on koodi haldamine ka arendusmeeskonnale kergem.

Järgnevalt on välja toodud kõik sammud käesolevas bakalaureusetöös käsitletava probleemi lahendamiseks.

3.3.1 Primaarsete omanike määramine

Kuigi pääsuõigustele on võimalik omanikke juba määrata, siis on vaja lisada funktsionaalsus mis võimaldab määrata ka primaarset omanikku. Primaarse omaniku ülesandeks on inventuuride kontekstis antud pääsuõiguse inventeerimine, kui vastava pääsuõiguste süsteemi inventuur käivitatakse (ning kui inventuuri luues on kinnitajateks valitud pääsuõiguste primaarsed omanikud).

Primaarseid omanikke on vaja ka pääsuõiguste süsteemidele, kelle ülesandeks on kõik süsteemi kuuluvata pääsuõiguste inventeerimine, kui inventuur käivitatakse ning inventuuri kinnitajateks on valitud on süsteemide primaarsed omanikud.

Added approvers			
	Bankier, Kaspar	Remove primary	×
	Rebase, Yulia	Make primary	×
	Reial, Raili	Make primary	×
	Semm, Kärt	Make primary	×

Joonis 5. Primaarse omaniku määramine

3.3.2 Aken pääsuõiguste süsteemi inventuuri loomiseks

Joonisel 6 on näha aken pääsuõiguste süsteemi inventuuri loomiseks, mis on sarnane juhi inventuuri omaga, lisaks on veel kaks välja:

- Süsteem – otsinguväli, mille kaudu süsteemi otsida ning valida.
- Kinnitaja – valik, kes inventeerima hakkab, võib olla kas süsteemi primaarne omanik või õiguste primaarsed omanikud.

Mugavuse huvides saab süsteeme aknas korraga lisada mitu tükki, igale süsteemile luuakse eraldi inventuur. Valitud süsteemide juures on kuvatud, kas süsteemil endal on primaarne omanik määratud ning kas süsteemi õigustel on primaarsed omanikud määratud. Kui kinnitajaks on valitud süsteemi primaarne omanik, ning valitud süsteemil (või süsteemidel) on süsteemi primaarne omanik puudu, siis pole inventuuri (või inventuuride) loomine võimalik.

Create system revision

Period 21.04.2021 until 29.04.2021

Reminder frequency 5

Occurrence 2

Country Baltic

System	System primary owner	Access rights primary owners
ART Tool	Available	Missing

ART Tool

Re-certifier System primary owner Access rights primary owners

Contact email kaspar.bankier@seb.ee

Cancel Create

Joonis 6. Süsteemi inventuuri loomise aken

3.3.3 Vaade inventuuris osalevale töötajale

Joonisel 7 on näha inventuuri vaade töötaja jaoks. Seal on kuvatud kõik süsteemid, mille kohta parasjagu inventuur on käimas. Olemas on ka filtrid (inventeeritud süsteemid, inventeerimata süsteemid, kõik süsteemid).

Iga süsteemi all on nimekiri pääsuõigustest, mida töötaja ülevaatama peab.

System recertification

Show not certified

Show certified

Show all

linkserver

Access right	Type	Description	Users
▶ amlwc	group		13
▶ arms	group		2
▶ audit	group		6
▶ backoff	group		16
▶ backrw	group		1
▶ base12	group	Krediidiriskikeskuse töötaja tehtud base12 failide asukoht (liisingu otsekulu ja vara müük) DWsse laadimiseks	4

Joonis 7. Inventuuri vaade töötajale

Joonisel 8 on näha avatud pääsuõiguse kohta täpsem ülevaade – mis rollidesse antud pääsuõigus kuulub, mis pääsuõigused on antud pääsuõigusest sõltuvad ning mis töötajatele antud pääsuõigus määratud on.

Rollidesse kuuluvus ning sõltuvused on ainult informatiivsed, kinnitada (*keep* või *remove*) saab ainult töötajaid – täpsemalt töötajaid, kellel pole antud pääsuõigus saadud läbi rolli.

▶ elukas group 10

▶ Roles (2)

Role	Description	Users	Action
Aktuaar	SEB Elu- ja Pensionikindlustuse aktuaari tööks vajalikud õigused Elukindlustuse rakenduses, NBSX-is ja CRM-is.	3	KEEPING
Accountant of life insurance	SEB Elu- ja Pensionikindlustuse raamatupidajale vajalikud õigused.	3	KEEPING

▶ Dependencies (2) ⓘ

Main access right	Dependant access right	Action
group elukas	Ldap: group elukas	KEEPING
group elukas	Active Directory: group AG-LEE-elukas_RW	KEEPING

▶ Employees (10)

Name	Username	Unit	Position	Active since	Request	Relation	Action
Ivo Kukk	iff	IT arenduse osakond	IT arendusjuht	11.06.2009	import		keep remove
Egris Mõttus	e90egmo	IT arenduse osakond	Rakenduse administraator	10.11.2014	18142		keep remove
Georgi Suikanen	S6536B	Müügi- ja turundusvaldkond	Analiütik	23.07.2018	149867		REMOVING ×
Toomas Tuuling	t10totu	Markets lahenduste arenduse osakond	Software Developer	11.06.2009	import		KEEPING ×

Joonis 8. Pääsuõiguse täpsem ülevaade

Kui kõik töötajad on kinnitatud, siis saab pääsuõiguse lõplikult kinnitada. Peale seda enam muudatusi teha ei saa.

3.3.4 Taotluste loomine

Peale pääsuõiguse lõplikku kinnitamist luuakse taotlused nendele töötajatele, kellelt pääsuõigus eemaldamiseks märgiti. Iga töötaja jaoks tehakse eraldi taotlus, kuid taotlused grupeeritakse ühte kogumisse – nii on kasutajal mugav näha, mis taotlused täpselt tehti (Joonis 9).

Requests Batch #2637

Details	Requests	Access Rights and Roles
Request #	Employee Name	Request Status
262589	Georgi Suikanen	Confirmed

Joonis 9. Taotluste kogum (ühe taotlusega)

3.3.5 Teavitused

Kasutajaõiguste registri administratiivsel poolel on võimalik seadistada teavitusi, mis inventuuri käivitumisel automaatselt meilidena välja saadetakse, neile töötajatele, kes peavad pääsuõigusi üle vaatama. Teavitusi saadetakse välja inventuuri loomisel määratud intervalliga (*reminder frequency*).

Samuti kuvatakse kasutajaõiguste registri päises sõnum, mis annab töötajale märku, et tal on inventuur millega tegelema peab.

3.3.6 Vaade inventuuri haldamiseks

Inventuuri haldamise vaates on administratiivsel poolel võimalik näha pääsuõiguste inventeerimise staatust, samuti saab seal pääsuõigusi inventuurist välja arvata (*close*). Vajaduse korral saab pääsuõigusi kellelegi teisele töötajale üle vaatamiseks määrata (*reassign*).

Genereerida saab ka XLSX (Excel-i tabeli vorming) vormingus raportit (Joonis 12), seda ühe pääsuõiguste ülevaataja (*reviewer*) inventuuri läbimise staatuse kohta.

Revision

[Back](#)

[Approvals](#) Details

Select reviewer [Generate xls report](#)

[REASSIGN](#) [CLOSE](#) Selected items to reassign or close: 1 Search: Show entries

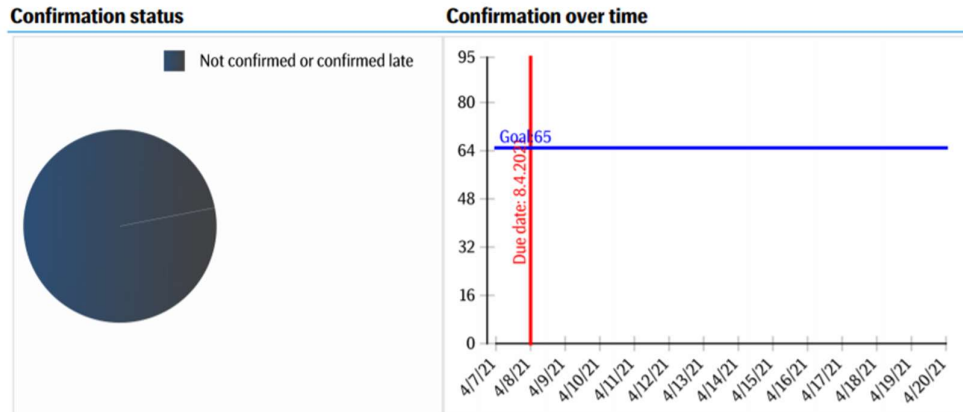
<input type="checkbox"/>	Review status	Reviewer	Access right	Unit	
<input checked="" type="checkbox"/>	Under review	Kaspar Bankier	liisu		No extra details
<input type="checkbox"/>	Under review	Kaspar Bankier	card	Kesksüsteemide arenduse osakond	No extra details
<input type="checkbox"/>	Under review	Kaspar Bankier	ep	Kliendandmete haldamise ja arvelduste osakond	No extra details

Joonis 10. Inventuuri haldamise vaade

3.3.7 Raportid

Raporte on võimalik ka koostada kõigi pääsuõiguste ülevaatajate inventuuri läbimise staatuse kohta, seda kas PDF (*Portable Document Format*) vormingus (Joonis 11) või XLSX (Joonis 12) vormingus.

System revision status report (linkserver) 7.4.2021 - 8.4.2021



Detailed overview

Approver	Unit	Profession	Total	Confirmed % 100%	Confirmed 1	Confirmed late 1	Not Confirmed 64
Kaspar Bankier				1%	1	1	64
group	liisu				Not approved		
	Andme- ja telefoniside osakond	Network Administrator	Ivo Lindegren		ivo		NOT REVIEWED
	Andmebaaside ja integratsiooni osakond	Andmebaaside administraator	Teet Jõhverd		teetj		NOT REVIEWED
	Andmebaaside ja integratsiooni osakond	Kesküsteemide ekspert	Rein Rüüsak		rein		NOT REVIEWED

Joonis 11. Raport PDF vormingus

Approver	Approver unit	over profe	Access right	Approved	Employee unit	Employee profession	Employee	Username	Status
Kaspar Bankier			group: amlw	Not approved	Turbekeskus	Turbejuht	Tarmo Kährik	e90taka	NOT REVIEWED
Kaspar Bankier			group: backoff	Not approved			Siim Kängsepp	S44139	NOT REVIEWED
Kaspar Bankier			group: backoff	Not approved	Markets lahenduste arenduse osakond	IT Team Lead	Tõnu Tomann	t10toto	NOT REVIEWED
Kaspar Bankier			group: backrv	Not approved			Siim Kängsepp	S44139	NOT REVIEWED
Kaspar Bankier			group: cardprep	Not approved			Grigori Ilkevits	S66169	NOT REVIEWED
Kaspar Bankier			group: cardprep	Not approved	Kesküsteemide arenduse osakond	Software Developer	Sergei Pivovarov	sergeip	NOT REVIEWED
Kaspar Bankier			group: cardprep	Not approved	Pangakaartide grupp	Arendusjuht	Piret Kurval	e90piku	NOT REVIEWED
Kaspar Bankier			group: cardprep	Not approved	Pangakaartide grupp	Tootejuht	Helle-Reet Kuningas	S12113	NOT REVIEWED
Kaspar Bankier			group: cardvalm	Not approved			Grigori Ilkevits	S66169	NOT REVIEWED
Kaspar Bankier			group: cardvalm	Not approved	Kesküsteemide arenduse osakond	Analyst	Sirje Tikan	e90siti	NOT REVIEWED

Joonis 12. Raport XLSX vormingus

3.3.8 Konsool

Selleks, et inventuurid õigel kuupäeval algaksid ja sulguksid ning toimuksid muud inventuuri seisuga kontrollimisega seotud tegevused, kasutakse cron-i, mis käivitab automaatselt PHP skriptis sisalduva vastava käskluse. Testimise otstarbel saab käsklust käivitada ka konsoolist käsitsi (Joonis 13).

```
[s5407c@lisd-riiull oigus]$ php riul-cli.php revisions
Checking assigned rights validity (status) for ongoing revisions
=====
- Checking for Revision with ID "188".
- Finished check for Revision with ID "188".
- Checking for Revision with ID "189".
- Finished check for Revision with ID "189".
- Checking for Revision with ID "190".
- Finished check for Revision with ID "190".
Right status validation check finished.

Checking for revisionApprovals with 0 assignable rights left to approve
=====
Zero check for assignable rights completed.

[s5407c@lisd-riiull oigus]$
```

Joonis 13. Inventuuride käskluse käivitamine konsooli kaudu

3.4 Koodinäited

3.4.1 Interaktiivsus

Kasutajamugavuse huvides kasutatakse inventuuri kinnitamiseks (kui ka muudeks interaktiivseteks toiminguteks, mille jaoks ei ole vajalik terve veebilehe uuesti laadimine) AJAX-i tehnikaid – tehakse asünkroonseid päringud kasutajaõiguste API-le. (Joonis 14). Selle tarbeks on kasutusel JavaScript-i teek jQuery.

Kuigi tänapäeval on võrreldes jQuery-ga populaarsust kogumas paljud JavaScript-i raamistikud, siis autor hindab, et antud lahenduse jaoks ei ole eraldi raamistiku kasutamine vajalik – ka ainult jQuery-st piisab antud lahenduse jaoks, sest äriloogika on rakenduse tasandil ning sellega on autoril ka palju kogemust.

Kasutajaõiguste registri arenduses on kaugemas tulevikus plaan kasutama hakata AngularJS raamistikku, mida ka ettevõttes mõningad lahendused juba kasutavad.

Päringutega tegeleb Slim raamistikul tuginev ruuter, mis vastavalt kasutajate päringutele suhtleb kontrollritega ning vajadusel kontrollib kasutaja luba mingi tegevuse sooritamiseks (Joonis 15).

```

$('#mySystems').on('click', 'a.myAccessRight.approve', function (event) {
  event.preventDefault();
  event.stopPropagation();
  if (!$('this').hasClass('disabled')) {
    let acceptButton = $(this);
    let openedTable = acceptButton.closest('.accessRightDetails');
    let approvalRow = acceptButton.closest('.approvalRow');
    let revisionApprovalId = acceptButton.data('revision-approval-id');
    let employeeId = acceptButton.data('employee-id');
    showLoaderOverlay(openedTable[0]);
    $.ajax({
      async: true,
      type: 'POST',
      url: apiUrl + 'assignedRights/system/verifyRevision',
      data: {
        'employeeId': employeeId,
        'revisionApprovalId': revisionApprovalId,
      },
      statusCode: {
        400: function (responseObject) {
          hideLoaderOverlay(openedTable[0]);
          tb_show(
            '',
            '#TB_error?width=300&height=300&autoscale=1',
            JSON.parse(responseObject.responseText)
          );
        },
      },
    })
    .fail(function () {
      tb_show(
        '',
        '#TB_error?width=300&height=300&autoscale=1',
        'Couldn\'t save the revision. Refresh and try again or
contact Service Desk.'
      );
      acceptButton.addClass('disabled');
      acceptButton.show();
      return false;
    })
    .success(function () {
      loadingMessage.addSavingTextRowAfter(approvalRow);
      approveRevision(acceptButton, REVISION_TYPE_SYSTEM);
    });
  }
});

```

Joonis 14. Inventuuri valideerimine ning kinnitamine

```
$route->group('/accessRight', function () use ($route) {
    $route
        ->post('/{rightId}/changePrimaryOwner/{employeeId}',
AccessRightController::class . ':changePrimaryOwner')
        ->add(new ApiAuthorizationMiddleware(Permission::MANAGE_RIGHT));
});
```

Joonis 15. Pääsuõiguse primaarse omaniku muutmise päringuga tegelemine router-is

3.4.2 Kontrollerid

Ruuteri kaudu kutsutakse välja esitlustasemesse kuuluvatest kontrolleritest meetodeid.

Kontroller täidab järgnevaid funktsioone:

- Kasutaja edastatud andmete esialgne valideerimine (Joonis 16),
- Andmete kuvamine Twig-i malle kasutades (Joonis 16),
- Suhtlemine teenustega.

```

public function revisionDetails(Request $request, Response $response, $args =
[])
{
    $revisionId = $args['id'];
    $type = strtoupper($args['type']);

    /** @var Revision $revision */
    $revision = $this->entityManager->find(Revision::class, $revisionId);

    if (!$this->revisionService->isValidType($type) || empty($revision) ||
$revision->isDeleted()) {
        $this->flash->addMessage('error', $this->translator-
>get('revision.error.detailsNotFound'));
        return $response->withRedirect($this->router-
>pathFor('revision.manager.index'));
    }

    switch ($type) {
        case Revision::TYPE_SYSTEM:
            $system = $revision->getSystem();
            return $this->render($response, 'revision/system/details.twig', [
                'revision' => $revision,
                'systemName' => $system->getName(),
                'systemPrimaryOwnerExists' => $this->approverService-
>systemHasPrimaryOwner($system),
                'systemAccessRightsPrimaryOwnersExist' => $this-
>approverService->systemRevisionAccessRightsHavePrimaryOwners($system),
                'type' => strtolower($type)
            ]
            );
        }
    }
}

```

Joonis 16. Kontrolleri funktsioon inventuuri haldusvaate kuvamiseks

3.4.3 Twig-i mallid

Kasutajale andmete kuvamiseks kasutatakse esitlustasandisse kuuluvaid Twig-i malle. (Joonis 17).

```

<td colspan="4">
  <table class="mt20 mb10">
    <tr>
      <th>{{ trans('recertification.system.table.header.role.name')
    }}</th>
      <th>{{
    trans('recertification.system.table.header.role.description') }}</th>
      <th>{{ trans('recertification.system.table.header.role.users')
    }}</th>
      <th>{{ trans('recertification.system.table.header.role.action')
    }}</th>
    </tr>
    {% if roles is defined and roles is not null and roles|length > 0 %}
      {% for role in roles %}
        <tr class="total normal">
          <td>{{ role.name }}</td>
          <td>{{ role.description }}</td>
          <td>{{ role.userCount }}</td>
          <td><p class="mt0 accept message left green bold
    nowrap">{{ trans('recertification.system.role.message.keep')|upper
    }}</p></td>
        </tr>
      {% endfor %}
    {% endif %}
  </table>
</td>

```

Joonis 17. Pääsuõigustega seotud rollide kuvamise Twig-i mall

3.4.4 Teenused

Rakenduse tasandisse kuuluvates teenustes paikneb kasutajaõiguste registri äriloogika. Teenused suhtlevad repositooriumitega ning edastavad andmeid kontrolleritele. Joonisel 18 on kujutatud funktsioon süsteemi inventuuri loomiseks, loomisel kasutatakse läbi *mapper*-i tehtud DTO-d (*Data Transfer Object*).

```

public function createSystemRevisions(array $data): array
{
    $revisions = [];
    $dto = RevisionMapper::toCreateRevisionDTO(Revision::TYPE_SYSTEM, $data);
    foreach ($data['system'] as $system) {
        /** @var System $system */
        $system = $this->systemService->getById(
            $system
        );
        if (is_null($system)) {
            throw new Exception("System does not exist!");
        }
        if ($system->getStatus() != System::STATUS_IN_USE) {
            throw new Exception("System is not in use!");
        }
        $dto->setSystem($system);
        try {
            $revision = $this->createRevisionByType($dto,
Revision::TYPE_SYSTEM);
        } catch (Exception $exception) {
            $this->logger->error($exception->getMessage(), $exception-
>getTrace());
            throw ApiInternalException::InternalError(
                "Something went wrong. Revision storing failed. Please try
again later"
            );
        }
        $revisions[] = $revision;
    }
    return $revisions;
}

```

Joonis 18. Teenuse funktsioon süsteemi inventuuri loomiseks

3.4.5 Mapper ja DTO

Mapper-i ülesandeks on kasutaja edastatud andmete põhjal (POST päringu massiiv) luua objekt, mida edastisteks toiminguteks mugav kasutada on, ehk DTO. Sellega sooritatakse tegevusi läbi repositooriumi andmete andmebaasi salvestamiseks.

3.4.6 Repositooriumid

Andmetasandisse kuuluvad repositooriumid suhtlevad andmebaasiga, sealt andmeid väljastades või salvestades. Repositooriumites on kasutusel Doctrine-i QueryBuilder, millega saab andmebaasi mugavalt PHP kaudu päringuid teha, eeliseks on halvemini hallatavate pikkade SQL-lausetete kirjutamise puudumine. QueryBuilder väljastab andmebaasi tabelile vastavaid objekte, mitte tavalisi kirjeid ridadena.

```

public function getRevisions(array $searchBy, array $groupBy = [], array
$orderBy = []): array
{
    $qb = $this->getEntityManager()->createQueryBuilder()
        ->select('r')
        ->from(Revision::class, 'r', 'r.id');
    $qb = $this->searchBy($qb, $searchBy);
    $qb = $this->groupBy($qb, $groupBy);
    $qb = $this->setOrderBy($qb, $orderBy);
    return $qb->getQuery()->getResult();
}

```

Joonis 19. Kriteeriumitele vastavate inventuuride andmebaasist väljastamine kasutades QueryBuilder-it

3.4.7 Raportid

Raportite genereerimise jaoks kasutatakse BIRT-i. Selleks eelnevalt genereeritakse XML-vormingus fail, mille põhjal lõplik raport genereeritakse (Lisa 2).

3.5 Testimine

Kasutajaõiguste registri arendusmeeskonnas ei rakendata ressursside nappuse tõttu koodi testimisel automaattestimist – nimelt on arendusmeeskond väga väike ning kõrgem prioriteet on muudel tööülesannetel. Siiski on automaattestimise vajalikkus mitmel korral üles kergitatud ning tulevikus plaanitakse seda rakendada. Sellegipoolest tehakse praegu kõik selleks, et *live* keskkonda jõuaksid üles ainult täielikult töötavad lahendused. Lahenduste teekond *live* keskkonda on järgnev:

1. Valminud lahenduse vaatavad üle kõik arendusmeeskonna liikmed ning teevad vajadusel kommentaare muudatusteks.
2. Kommentaaridele vastavalt viiakse sisse muudatused.
3. Kui kõik on töökorras, siis laetakse lahendus *test* keskkonda, kus lahendust proovib administratiivne pool. Juhul kui nemad leiavad midagi, mis on katki või mida peaks muutma, korratakse eelnevaid samme.
4. Lahendus laetakse *live* keskkonda.

Käesoleva lahenduse osade testimine oli esialgu aeganõudev – mitmel korral esines juhtumeid, kus autoril tuli mingi osa ümber teha, peamiselt selle tõttu, et arusaam kasutajaõiguste registri tööst oli puudulik.

3.6 Probleemid

Kõige suuremaks probleemiks lahenduse väljatöötamisel kujunes viimane samm – raportite genereerimise funktsionaalsuse loomine. Kuigi autoril on kogemus PHP-s programmeerimisega (mida lahenduse loomine enamjaolt vajas), siis raportite jaoks pidi kasutama tarkvara, millega autoril kogemus puudus.

Töö käigus tuli ilmsile ka probleem, et mõni süsteem on liiga suur, et eeldada sellesse kuuluvate pääsuõiguste üksikasjalikku üle vaatamist. Selle lahendamiseks lahendamiseks oli vajalik luua võimalus pääsuõigusi vaikimisi inventuuri mittekuuluvaks märkida. Samuti inventuuri mitte kaasata pääsuõigusi, mida pole määratud ühelgi töötajale, mis ei kuulu ühtegi rolli ning millel pole ühtegi sõltuvust. Selle tulemusel on suurte süsteemide (ligi kümme tuhat pääsuõigust) inventeerimine vähem aeganõudev protsess.

Üldiselt ei olnud töö käigus suuri takistusi, kuigi kasutajaõiguste registriga esialgu tuttavaks saamine oli autorile raske, peamiseks põhjuseks oli dokumentatsiooni puudumine – vajalik oli arendusmeeskonna ning administratiivse poole pidev juhendamine.

4 Tulemused

4.1 Hinnang

Autor hindab, et vaatamata esinenud probleemidele on saadud tulemus hea – loodud on täielikult funktsionaalne lahendus mis katab kõiki ettevõtte nõudeid.

Töö käigus õppis autor tundma uusi tehnoloogiad ning sai tuttavamaks tarkvaraarenduse protsessiga suuremas ettevõttes, lisaks omandas autor arvestatava pädevuse kasutajaõiguste registri arendamises ja kasutamises.

4.2 Tagasiside

Kasutajaõiguste registri administratiivsele poolelt (nemad inventuuridega peamiselt tegelevad) kogutud tagasiside on olnud positiivne – teeb nende tööd kergemaks, sest ilma selle lahenduse puudumiseta peaks inventuure tegema käsitsi, kasutades Excel-it.

4.3 Tuleviku arendused

Kuigi loodud lahendus on täielikult funktsionaalne, kuid siiski võib tulevikus administratiivsel poolel sellega seoses veel soove tekkida, mis jäävad autorile lahendada.

Lisaks juhi ning pääsuõiguste süsteemide inventeerimisele on vaja veel inventeerida ka rolle, järgmiseks ülesandeks on see lahendus luua. Kuna autor on tuttavamaks saanud kasutajaõiguste registri tööga, siis on selle lahenduse loomine lihtsam. Lisaks saab selle tarbeks kasutada pääsuõiguste süsteemide inventeerimise lahenduse osasid, seega tehtava töö maht on väiksem.

Autor hindab ka, et tulevikus oleks vajalik koostada kasutajaõiguste registrile ammendav dokumentatsioon, arvestades selle suurt mahtu ning keerukust.

Kokkuvõte

Käesoleva bakalaureusetöö eesmärk oli luua ettevõttele AS SEB Pank seal kasutatavale kasutajaõiguste registrile lahendus pääsuõiguste süsteemide inventeerimiseks, ettevõtte poolsete nõuete alusel.

Töö käigus tehtud analüüs andis ülevaate ettevõttes kasutatavast kasutajaõiguste registrist ning sellest, kui oluline on töötajate pääsuõiguste kontrollimine ning millised on võimalikud ohud, kui töötajate pääsuõiguste haldamine on puudulik. Lahenduse peatükk kirjeldab kasutajaõiguste registri arhitektuuri ning seal kasutatavaid tehnoloogiaid, samuti on antud ülevaade loodud pääsuõiguste süsteemide inventuuri lahendusest ning arenduse käigus esile tõusnud probleemidest.

Lahenduse väljatöötamist saab pidada edukaks – see täidab kõik vajalikud nõuded ning on täielikult töövalmis.

Kasutatud kirjandus

- [1] AS SEB Pank, „Põhiväärtused,“ [Võrgumaterjal]. Available: <https://www.seb.ee/seb/ettevotest/pohivaartused>.
- [2] Techgardens, „Top Eight Most Vulnerable Industries For Cyber Attack,“ [Võrgumaterjal]. Available: <https://techgardens.com/top-eight-vulnerable-industries-cyber-attack/>.
- [3] Atlassian, „Sprints,“ [Võrgumaterjal]. Available: <https://www.atlassian.com/agile/scrum/sprints>.
- [4] D. Radigan, „Four agile ceremonies, demystified,“ [Võrgumaterjal]. Available: <https://www.atlassian.com/agile/scrum/ceremonies>.
- [5] S. v. Rooden, „Product Backlog Refinement explained (2/3),“ [Võrgumaterjal]. Available: <https://www.scrum.org/resources/blog/product-backlog-refinement-explained-23>.
- [6] K. Eby, „What's the Difference? Agile vs Scrum vs Waterfall vs Kanban,“ 15 Veebruar 2017. [Võrgumaterjal]. Available: <https://www.smartsheet.com/agile-vs-scrum-vs-waterfall-vs-kanban>.
- [7] Ponemon Institute, „Corporate Data: A Protected Asset or a Ticking Time Bomb?,“ Detsember 2014. [Võrgumaterjal]. Available: <https://info.varonis.com/hs-fs/hub/142972/file-2194864500-pdf/ponemon-data-breach-study.pdf>.
- [8] Phishing.org, „Phishing Examples,“ [Võrgumaterjal]. Available: <https://www.phishing.org/phishing-examples>.
- [9] Logi Analytics, „3-Tier Architecture: A Complete Overview,“ [Võrgumaterjal]. Available: <https://www.jinfonet.com/resources/bi-defined/3-tier-architecture-complete-overview/>.
- [10] Nitrosphere, „2-Tier vs. 3-Tier Application Architecture?,“ [Võrgumaterjal]. Available: <https://nitrosphere.com/uncategorized/2-tier-vs-3-tier-application-architecture-could-the-winner-be-2-tier-2/>.
- [11] The PHP Group, „PHP: Hypertext Preprocessor,“ [Võrgumaterjal]. Available: <https://www.php.net/>.
- [12] Stack Exchange, „2020 Developer Survey,“ [Võrgumaterjal]. Available: <https://insights.stackoverflow.com/survey/2020>.
- [13] Q-Success, „Usage statistics of PHP for websites,“ [Võrgumaterjal]. Available: <https://w3techs.com/technologies/details/pl-php>.
- [14] SensioLabs, „Twig - The flexible, fast, and secure template engine for PHP,“ [Võrgumaterjal]. Available: <https://twig.symfony.com/>.
- [15] Slim, „Slim Framework,“ [Võrgumaterjal]. Available: <https://www.slimframework.com/>.
- [16] A. Njenga, „10 Popular PHP frameworks to consider,“ November 21 2018. [Võrgumaterjal]. Available: <https://raygun.com/blog/top-php-frameworks/>.
- [17] Doctrine, „Doctrine: PHP Open Source Project,“ [Võrgumaterjal]. Available: <https://www.doctrine-project.org/>.

- [18] Tina, „Introduction to Object-relational mapping: the what, why, when and how of ORM,“ 19 November 2020. [Vörgumaterjal]. Available: <https://dev.to/tinazhouhui/introduction-to-object-relational-mapping-the-what-why-when-and-how-of-orm-nb2>.
- [19] Cake Software Foundation, „Introduction,“ [Vörgumaterjal]. Available: <https://book.cakephp.org/phinx/0/en/intro.html>.
- [20] The Eclipse Foundation, „Birt,“ [Vörgumaterjal]. Available: <https://www.eclipse.org/birt/>.
- [21] S. K., „Cron Job: A Comprehensive Guide for Beginners 2021,“ 2 Märts 2021. [Vörgumaterjal]. Available: <https://www.hostinger.com/tutorials/cron-job>.
- [22] OpenJS Foundation, „jQuery,“ [Vörgumaterjal]. Available: <https://jquery.com/>.

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks¹

Mina, Kaspar Bankier

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „AS SEB Pank pääsuõiguste süsteemide inventeerimine“, mille juhendaja on Meelis Antoi
 - 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.

26.04.2021

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 loomingu tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtjaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtjaja jooksul ei kehti.

Lisa 2 – Osa genereeritud XML-failist raporti loomiseks

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:SystemRevisionReviewerReport
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.seb.ee/riiul/report report.xsd"
xmlns:tns="http://www.seb.ee/riiul/report">
  <tns:Revision tns:Start="2020-10-13" tns:Due="2021-10-29"
tns:Type="SYSTEM"/>
  <tns:Approval tns:Status="APPROVED" tns:Approved="2020-10-22">
    <tns:Approver tns:Id="13084" tns:FirstName="Kaspar" tns:LastName="Bankier"
tns:MainUsername="s5407c"/>
    <tns:AccessRight tns:Id="24427" tns:SystemId="116" tns:TypeId="1"
tns:Name=" SEB-EE-ACCOUNT-MANAGER" tns:Description="Wall Street Suite version
7.4" tns:SystemName="WSS" tns:TypeName="group"/>
    <tns:ReviewableItemList>
      <tns:Item tns:Reviewed="2020-10-22" tns:UserName="s8843b"
tns:Status="REMOVE" tns:FirstName="Indrē" tns:LastName="Šinkūnaitē"/>
      <tns:Item tns:Reviewed="2020-10-22" tns:UserName="s8913b"
tns:Status="REMOVE" tns:FirstName="Justas" tns:LastName="Semenavičius"
tns:Unit="Baltijos rinkos vertybinių popierių ir finansų rinkų operacijų
grupė" tns:Profession="Process Area Specialist"/>
      <tns:Item tns:Reviewed="2020-10-22" tns:UserName="s3128B"
tns:Status="REMOVE" tns:FirstName="Aistė" tns:LastName="Mackevičiūtė"
tns:Unit="Baltijos rinkos vertybinių popierių ir finansų rinkų operacijų
grupė" tns:Profession="Process Area Specialist"/>
      <tns:Item tns:Reviewed="2020-10-22" tns:UserName="s26927"
tns:Status="REMOVE" tns:FirstName="Anželika" tns:LastName="Kozlovskaja"
tns:Unit="Baltijos rinkos vertybinių popierių ir finansų rinkų operacijų
grupė" tns:Profession="Process Area Specialist"/>
    </tns:ReviewableItemList>
  </tns:Approval>
</tns:SystemRevisionReviewerReport>
```