VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
INFORMATIKOS INSTITUTAS

Architektūriniai požiūriai

Architectural viewpoints

Programų sistemų architektūros ir projektavimo laboratorinis darbas

Atliko: Matas Savickis (parašas)

Darbo vadovas: Rimantas Kybartas, Partn. Prof., Dr. (parašas)

Recenzentas: (parašas)

Vilnius – 2020

TURINYS

1. Sistema

Žmonės turi daiktų, kuriuos nori parduoti, tačiau nežino kiek tiksliai jų parduodamas daiktas gali būti vertas. Sistema leidžia vartotojams parduoti daiktus aukciono principu. Vartotojas įdeda norimą daiktą į aukcioną nustatydamas mažiausią kainą už kurią sutiktų parduoti daiktą, nustato aukciono trukmę ir kiti sistemos parduotojai gali didinti daikto kainą iki nustatyto laiko. Sistema suteikia galimybę atsiskaityti už prekes elektroninio banko pervedimais ir kriptovaliutomis.

2. Suinteresuoti asmenys

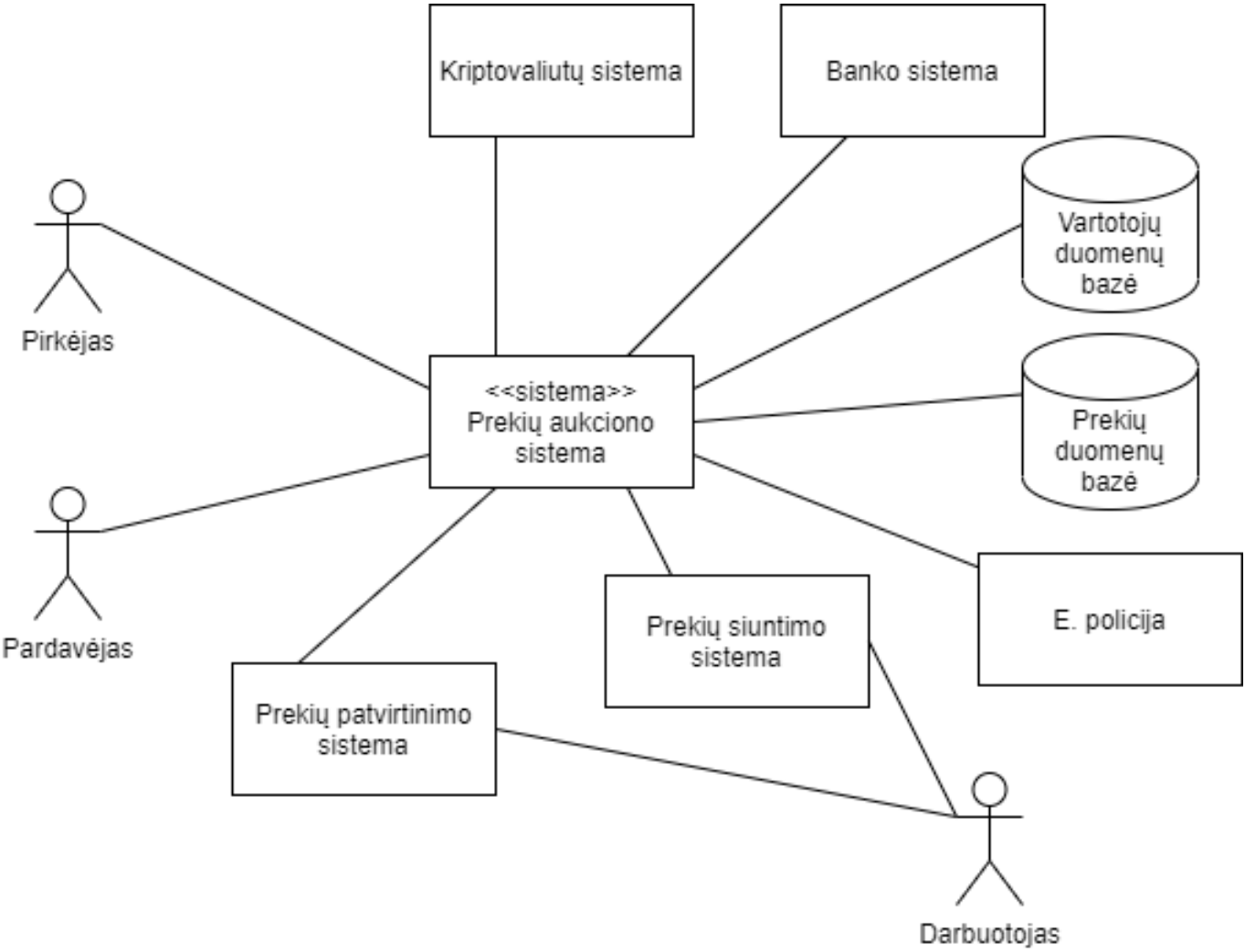
- Pirkėjai - vartotojai, kurie naudosis aukcionu siekdami parduoti prekę.
- Pardavėjai - vartotojai, kurie naudosis aukcionu siekdami nusipirkti prekę.
- Investuotojai - žmonės, kurie rems projekto įgyvendinimą finansiškai
- Programuotojai - žmonės, kurie kurs sistemą.
- Testuotojai - žmonės, kurie testuos sistemą.
- Policija - suinteresuota nelegalių daiktų pirkėjų ir pardavėjų identifikavimu.
- Lietuvos teismas - suinteresuotas nelegalių prekių pirkimu ir pardavimu, taip pat Lietuvos įstatymų laikymusi.
- Europos sąjunga - suinteresuota, kad sistema laikytusi europos sąjungos įstatymų ir reglamentų(BDAR)

3. Konteksto požiūrio taškas

3.1. Sistemos taikymo sritis

Vartotojas sistemoje įkelią savo skelbimą, kiti vartotojai dalyvauja aukcione ir didžiausią kainą pasiūlęs vartotojas laimi aukcioną. Aukcioną laimėjęs žmogus perveda pinigus arba Bitcoin kripto valiutą į mūsų sistema, tuomet prekės pardavėjas išsiunčia prekę į mūsų biurą patikrinti ar prekė atitinka aprašymą. Biuro darbuotojui patvirtinus, kad prekė atitinka aprašymą sistema perveda pinigus pardavėjui jo pasirinktu būdu.

3.2. Konteksto požiūrio taško diagrama



1 pav. Aukciono sistemos konteksto požiūrio taško diagrama

3.3. Funkciniai reikalavimai

3.3.1. Pardavėjas reikalavimai

1. Pirkėjas turi galimybę įdėti prekę į aukcioną nurodydamas jos pradinę kainą, aukciono trukmę, aprašymą ir įkeldamas fotogtafiją.

2. Pirkėjas atšaukti aukcioną jam nepasibaigus taip nebeparduodant prekės.

3. Atsiradus pirkėjui, po aukciono pardavėjas turi prekę išsiųsti į aukciono sandelį per dvi darbo dienas.

4. Pirkėjas pardavęs prekę gali pasirinkti išmokėjimo būdą: pavedimas į sąskaitą, kriptovaliutas, aukciono sąskaitos papildymas.

3.3.2. Pirkėjas reikalavimai

1. Pirkėjas norėdamas dalyvauti aukcione turi įsidėti pinigų į aukciono sąskaitą.

2. Aukciono sąskaitą galima papildyti per elektroninį banką arba pervedant kripto valiutas į sistemos piniginę.

3. Pirkėjas gali siūlyti didesnę prekės kainą kol prekės aukcionas nepasibaigė.

4. Paskutinis aukščiausią kainą pasiūlęs pirkėjas laimi aukcioną.

5. Aukciono nugalėtojas gali sekti jam atkeliaujančia prekę.

6. Nugalėtojui negavus prekės jo pinigai pervedami į aukciono sąskaitą.

7. Pirkėjas gali komentuoti prie kiekvienos prekės.

8. Pirkėjas gali persivesti savo aukciono sąskaitą į savo kriptovaliutų piniginę arba į savo bankinę sąskaitą.

3.3.3. Prekių siuntimo reikalavimai

1. Pardavėjui atsiuntus prekę į aukciono sandėlį prekė yra patvirtinama aukciono darbuotojo ar siuntinys atitinka aukcione pateiktą prekės aprašymą ir nuotrauką.

2. Gavus įtartiną siuntinį aukciono darbuotojas informuoja policiją pateikdamas pirkėjo ir pardavėjo duomenis

3. Jeigu prekė neatitinka aprašymo ir fotografijos pinigai būna gražinami pirkėjui ir krepė yra išsiunčiama pardavėjui išperkamosios siuntos principu.

3.3.4. Banko reikalavimai

1. Sistemoje yra galimybė pervesti pinigus iš banko sąskaitos į aukciono sąskaitą.

2. Sistemoje yra galimybę gauti pinigus iš aukciono sąskaitos į banko sąskaitą.

3. Bankinės pranzakcijos yra vykdomos banklink paslauga.

3.3.5. Kriptovaliutų reikalavimai

1. Sistemoje yra galimybė pervesti kritovaliutas iš kripto piniginės į aukciono sąskaitą, kripto valiutos automatiškai konvertuojamos į eurus taikant papildoma mokestį.
2. Sistemoje yra galimybė pervesti pinigus iš aukciono sąskaitos į kriptovaliutų piniginę taikant papildomą mokestį.

3.3.6. Policijos reikalavimai

1. Policijai apie nelegalias prekes yra pranešama naudojanti e. Policija paslaugomis.

3.3.7. Teisiniai reikalavimai

1. Sistema veikia laikydamasi Lietuvos įstatymų.
2. Sistema veikia laikydamasi Europos įstatymų ir BDAR reglamento.

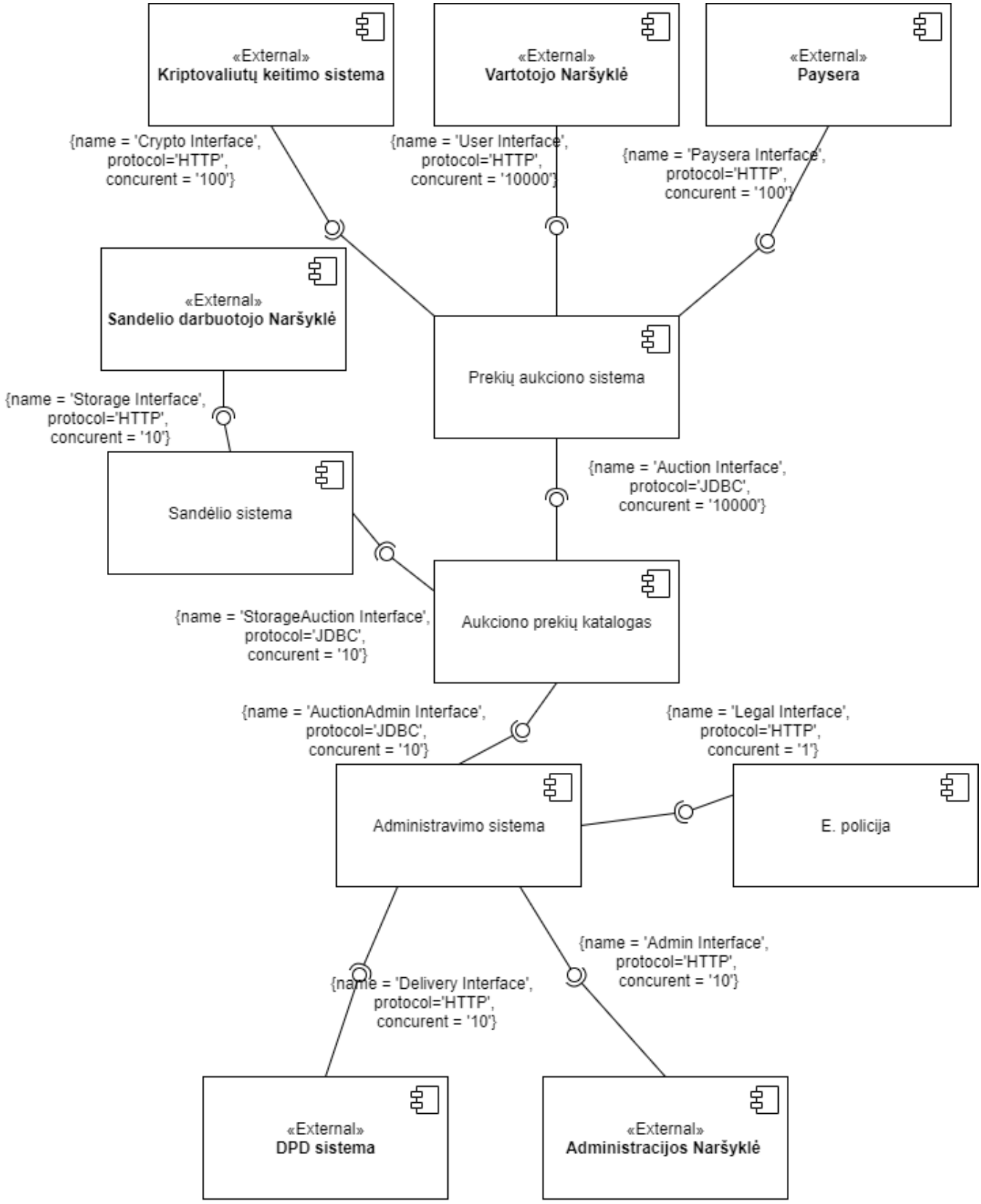
3.3.8. Bendri reikalavimai

1. Vartotojui paprašius jo duomenys yra pašalinami iš sistemos per mėnesį.
2. Vartotojas gali matyti savo pirkimų ir pardavimų istoriją.

4. Funkcinis požiūrio taškas

Sistema kuriama bandant išlaikyti komponentų atskirtį, sustojus veikti vienam sistemos komponentui, kiti komponentai neturi būti įtakojami. Sustojus „Prekių aukciono sistema” komponento veikimui vis dar veikia „Administravimo sistema” komponento veikimas ir taip toliau.

4.1. Komponentų diagrama



2 pav. Kompnentų diagrama

4.2. Interfeisų aprašai

Interfeiso pavadinimas	Crypto Interface
Aprašymas	Interfeisas atsakingas už vartotojų kripto valiutų pervedimus ir pinigų išgryninimą iš kripto valiutos į eurus

1 lentelė. Crypto Interface

Interfeiso pavadinimas	User Interface
Aprašymas	Interfeisas skirtas perduoti perduoti duomenis vartotojo naršyklei. Perduodami su aukcionu susije duomenys.

2 lentelė. User Interface

Interfeiso pavadinimas	Paysera Interface
Aprašymas	Skirta atlikti pavedimus pridedant pinigus į aukciono sąskaitą arba juos bandant išsiimti. Šis intefeisas taip pat skirtas pinigus pervesti į įmonės sąskaitą

3 lentelė. Paysera Interface

Interfeiso pavadinimas	Storage Interface
Aprašymas	Šio interfeisu naudojamasi perduoti duomenis sandelio darbuotojo naršyklei bei sandelio daruotojui pranešti apie blogas arba neatitinkančias prekes

4 lentelė. Storage Interface

Interfeiso pavadinimas	StorageAuction Interface
Aprašymas	Interfeisas skirtas komunikuoti su aukciono prekiu duomenu baze

5 lentelė. StorageAuction Interface

Interfeiso pavadinimas	Auction Interface
Aprašymas	Interfeisas skirtas komunikuoti su duomenų baze. Šioje vietoje aukcione atlikti pirkimai ir pardavimai užregistruojami duomenų bazėje.

6 lentelė. Auction Interface

Interfeiso pavadinimas	AuctionAdmin Interface
Aprašymas	Administratoriaus sąsajos bendravimo su aukciono duomenų baze. Čia administratorius gali matyti aukciono informaciją ir ją dalinai koreguoti

7 lentelė. AuctionAdmin Interface

Interfeiso pavadinimas	Legal Interface
Aprašymas	Šiame interfese administratorius perduoda reikalingą informacija e.Policijai apie nelegalias prekes siunčiamas aukcione

8 lentelė. Legal Interface

Interfeiso pavadinimas	Admin Interface
Aprašymas	Interfeisas per kuri administratorius pasiekią aukciono platformą per naršyklę

9 lentelė. Admin Interface

Interfeiso pavadinimas	Delivery Interface
Aprašymas	Interfeisas skirtas administracijai komunikuoti su pristatymu įmone DPD, atlikti siuntų paėmimą ir sekimą.

10 lentelė. Delivery Interface

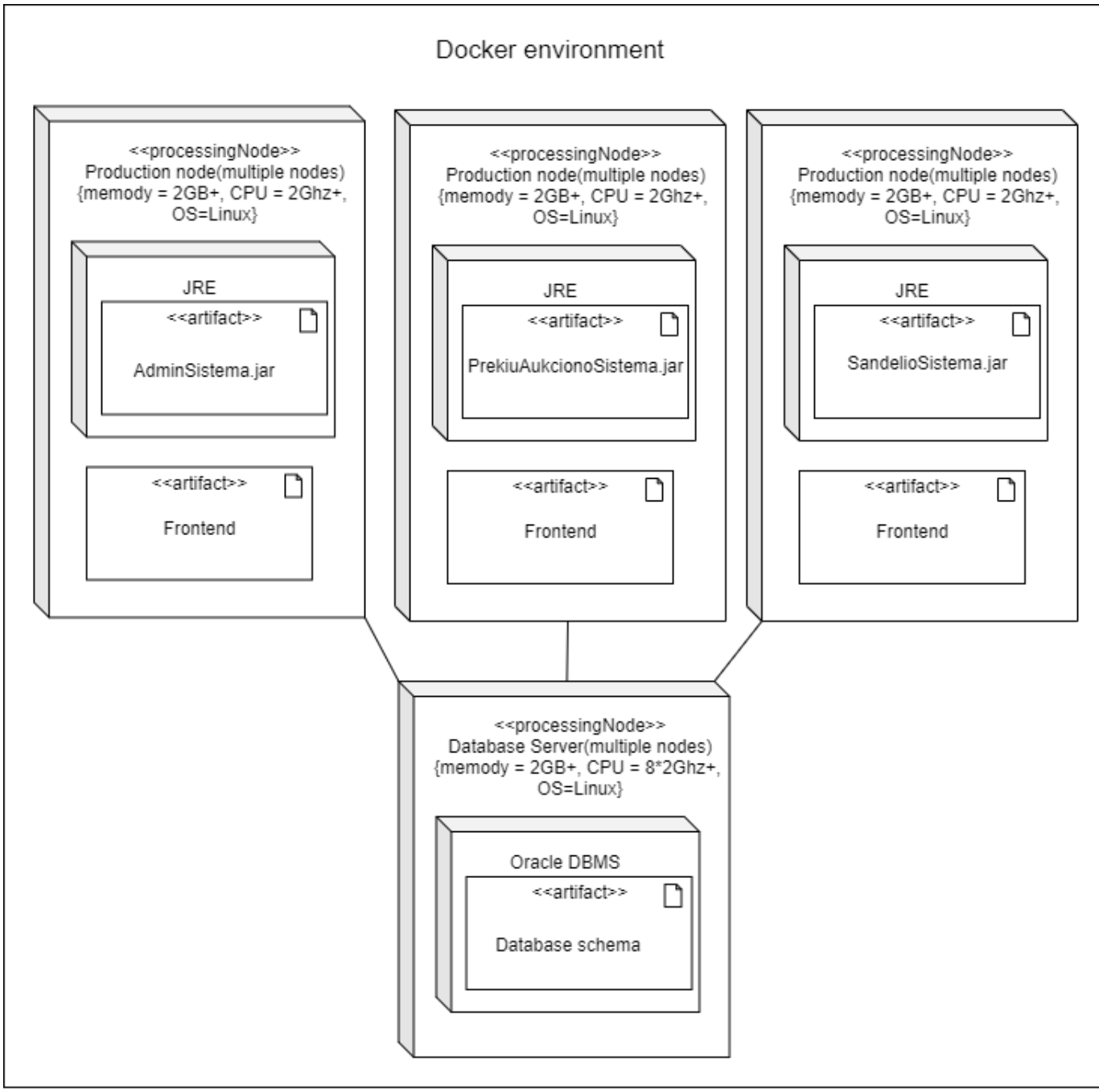
4.3. Procesai apimantys visą sistemą

Sistemoje vykdomas įvykių žurnalizavimas sekti vartotojo veiksus sistemoje ir registruoti sistemines klaidas. Šis procesas apima visus vidinius sistemos komponentus. Žurnalai saugomi sistemos serveryje.

5. Diegimo požiūrio taškas

Sistema yra išskirstyta į tris skirtingas produkcines aplinkas iš kurių kiekviena aplinka gali būti sukurta kelis kartus siekiant horizontalaus scale'inimo. Aplinkoje taip pat yra duomenų bazės mazgas, jo taip pat galima sukurti kelis mazgus siekiant paskirstyti apkrovas. Duomenu bazė tampa eventualy consistant. Produkcinėje aplinkoje yra backend jar failas, ir front end failai. Visos aplinkos veikia ant Linux operacinės sistemos o visi mazgai yra Docker aplinkoje.

5.1. Diegimo diagrama



3 pav. Kompnentų diagrama

5.2. Priklausomybių modelis

- JRE 1,8
- Orable DBMS 11
- Linux
- Node.js
- Spring Boot
- Docker

6. Operatyvinis požiūrio taškas

6.1. Diegimas ir migracija

Diegimas vykdomas sukuriant atitinkamus mazgus debesijos aplinkoje. Norint paleisti produkcijos Java projektus komandinėje eilutėje reikia įrašyti mvn clean install -Pbuild Sistemos modulių veresijos kėlimui naudojama sudo apt-get install.

6.2. Configūracijos valdymas

Vidurnakti yra sukuriamas naujas žurnalizavimo failas sekti sekančios dienos įvykiams ir sisteminėms klaidoms. Vidurnakti atliekamas naujos versijos diegimas arba modulių bei bibliotekų update'inimas

6.3. Sistemos administravimas

Sistemą prižiūri vienas Fullstack programuotojas

7. Saugumo perspektyva

7.1. Konteksto požiūrio taško saugumo perspetyva

Išoriniai ryšiai ir su jai susijusios grėsmės

- Vartotojo sąsaja – į per vartotojo sąsaja gali prisijungti neautorizuotas vartotojas ir gauti vartotojo asmeninius duomenis bei siuntų pristatymo ir išsiuntimo adresus. Susiekti su administracija, kad būtų pakeičiamas siuntos adresas.
- Kriptovaliutos sistemos sąsaja – nekorektiškai siunčiant duomenis gali būti perimti ir kripto valiutos persiunčiamos į kitą piniginę
- Banko sistemos sąsaja – gresmė panaši kaip ir su kripto valiutomis, nekorektiškai siunčiant duomenis juos būtų galima perimti ir pinigai būtų siunčiami į kitą sąskaitą.
- Vartotojo duomenų bazė – gavus administratoriaus lygio prieeigą prie duomenų bazės būtų galima gauti visus asmeninius duomenis saugomus joje.
- Prekių duomenų bazė – panašiai kaip ir su vartotojo duomenų bazėmis gavus prieeiga būtų galima gauti duomenis apie siuntas ir taikant socialinės inžinerijos atakas perimtas tas siuntas ir pakeisti adresatus.
- E. policijos duomenų bazė – kenkėjiškai sistemai imitavus E. policijos sąsaja būtų galima perimti informaciją apie vartotojus bei paprašyti nelegalių siuntų atsiėmimo.
- Prekių siuntimo sistemos sąsaja – gavus prieeigą prekių siuntimo sąsajos būtų galima nukreipti siuntinius kitu adresu.
- Prekių patvirtinimo sistema – gavus prieeiga prie patvirtinimo sistemos būtų galima patvirtinti ir išiųsti nelegalias prekes.

Į šias sistemas galima įsilaužti socialinės inžinerijos, slaptažodžių perrinkimo ir vidurinio žmogaus atakos metodais.

7.2. Funkcinio požiūrio taško saugumo perspektyva

Saugumui svarbūs funkciniai elementai:

- Prekių aukciono sistema – Išorinė sąsaja bendraujanti su vartotojais ir pinigų valdymo sistemomis. Savarbu užtikrinti, kad pinigų ir kripto valiutų sistemos būtų saugiai pasiekiamos ir neįvyktu vidurio žmogaus atakų.
- Aukciono prekių sistema – Šio komponento sauguma užtikrinti saugiausia, nes kiti komponentai jungiantys prie šio komponento gali pasiekti pasiekti visus sistemos duomenis apie vartotojus ir prekes, todėl svarbu užtikrinti, kad sąsaja su kitais lementais kuriems siunčiama informacija, būtu saugi

- Sandelio sistema – šioje sistemoje svarbu užtikrinti, kad prekių siuntimo ir gavimo adresas nebūtų pakeistas, bei nebūtų nelegalios prekės nurodytos kaip legalios.
- Administravimo sistema – gavus prieeiga prie administratoriaus saršyklės būtų galima nusiųsti DPD prekių siuntų sistemai kitus adresus ir prekės būtų pristatytos į netinkamą adresą.

7.3. Diegimo požiūrio taško saugumo persketyva

Diegiant programinę įrangą yra svarbu ne diegti naujausios versijos programas, o diegti programas su stabiliomis ir patikrintomis versijomis. Kiekviena programa ir jos naudojamos versijos turi būto laikomos vidiniame įmonės repozitoriume, kad išvengti problemų jeigu programos kūrėjai nebepalaikyti senos versijos. Pačią naujausia versiją reiktų diegti tik tuo atveju jeigu joje išspręstos svarbios sistemos saugumo spragos. Diegimo požiūrio taške svarbu užtikrinti šiuos dalykus:

- Docker – svarbu palaikyti saugią ir stabilią versiją.
- Techninė įranga(CPU,GPU,Motherboard) – svarbu atnaujinti įrangos draiverius ir palaikiančia programinę įrangą.
- JRE – svarbu turėti saugią aplinkos versiją.
- Front-end – svarbu palaikyti saugią karkasų versija, analizuoti ar Front-end kodas nepriklauso nuo abeotino saugumo npm modulių, stengtis kad būtų kuo mažiau npm priklausomybių
- Duomenų bazė - svarbu turėti saugią duomenų bazės versiją.

Atnaujinant programos versiją turi būti paruoštas roll-back planas, jeigu įdiegta versija pasirodytų esą nestabili arba turinti saugumo spragų. Diegiant versijas svarbu turėti jas išsisaugojus savo sistemos repozitoriume, kad būtų sumažintas komunikavimas su internetu ir naujų failų siuntimasis, kad atveria daugiau saugumo spregų. Jeigu sistema bus kuriama debesijos aplinkoje saugiomis programų versijomis bus pasirūpinta debelies tiekėjo.

7.4. Bendra saugumo perspektyva

7.4.1. Resursai

Apie resursus ir jų įtaką saugumui aprašyta praeituose skirsniuose

7.4.2. Politika

Vartotojų grupės ir jų galimybė pasiekti sistemas:

- Vartotojas - netiesiogiai gali pasiekti prekių katalogo informaciją ir atlikdamas pirmikus arba pardavimus netiesiogiai keisti šią informaciją. Jeigu vartotojas sugeba pasiekti jam nepriskirta informacijos saugumo lygi už tai yra atsakingas sistemos administratorius.

- Darbuotojas - gali pasiekti Prekių aukciono katalogo sistemą, sandelio sistemą bei administravimo sistemą. Darbuotojas gali pasiekti visą informaciją esančia sistemoje tačiau negali koreguoti vartotojo ir prekių duomenų. Darbuotojas gali koreguoti prekės siuntimo būseną, bei gali pakeisti prekės legalumo būsena iš legalios į nelegalią, tačiau ne atvirkščiai.
- Sistemos administratorius - gali matyt ir keisti visus sistemos duomenis. Yra atskingas už netikamo turinio ir kenkėjimų naudotojų panaikinimą iš sistemos, pranešimą policijai apie nelegalias prekes bet prekės būsenos atstatymą iš nelegalios į nelegalią.

7.4.3. Mechanizmai

Užtikrinti saugumą bus įgyvendinti šie saugumo mechanizmai

- Vartotojams - registruojantis ir jungiantis prie sistemos vartotojas turės nurodyti pakankamo saugumo slaptažodį. Jungiantis prie sistemos vartotojas turės naudotis dviejų faktorių autetikacija. Slaptažodis turės bus keičiamas kas pusę metų. Iš vartotojo pusės nebus galimą siųsti perdaug užklausų iš vieno IP adreso arba prieeiga vartotojui bus laikinai apribota. Jungiantis prie sistemos vartotojas turės naudotis pakankamai saugios versijos naršyklę.
- Darbuotojams - Darbuotojams norint prisijungti prie sistemos reiktu prisijungti per VPN, trūrėti pakankamo saugumo slaptažodi kuris būtu keičiamas kas tris mėnesius bei turėti dviejų faktorių autentikacijos PIN kodo generatorių. Už isilaužimus į darbuotojo sistema atsakingas yra Administratorius
- Administratorius - tie patys reikalavimai kaip ir darbuotojui tik slaptažodis keičiamas kas mėnesį

7.4.4. Principai

Sistemoje laikomasi duomenų prieeigos mažinimo ir edukacijos principų. Vartotojui suteikti tik tiek prieeigos kiek jam reikia atlikti savo darbus ir ne daugiau. Kas pusę metų Darbuotojams ir administratoriams rodyti informacijos saugumo edukacinius video ir liepti praeiti testą apie infomaciją pateiktą edukaciniuose video. Vykdyti Phishing treniruotes kuomet sistemos vartotojams yra išsiunčiami nesaugios nuorodos taip skatinti vartotojų budrumą, o vartotojui paspaudus ant Phishinimo atakos nuorodos prašyto jo dar kartą peržiūrėti informacijos saugumo edukaciniu video. Saugumas yra užtikrinamas per geranorišką edukacija, o ne per baudimus.

7.5. Įsilaužimo protokolas

Įvykus isilaužimui į sistemą visas sistemos darbas yra nutraukiamas. Sistemos administratorius informuoja Nacionalinį kibernetinio saugumo centrą apie įvykusį įsilaužimą. Nustatoma sistema į kurią buvo įsilaužta ir atkūriami pakeisti duomenį, sumokama finansinė kompensacija jeigu vartotojas patyrė nuostolių dėl įsilaužimo ir ši suma neviršiją 5000 eurų. Visiems sistemos vartotojams liepiama pakeisti visus savo slaptažodžius. Sudaromas saugumo spragos ištaisymo planas. Pakeliama arba sumažinama programos versija jeigu tai padėtų saugumui.