TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Karl Kristjan Kalluste
163954IAPB

Euroopa makseteenuste direktiivil PSD2 põhineva makse algatamise teenuse loomine

Bakalaureusetöö

Juhendaja: Evelin Halling
PhD

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: Karl Kristjan Kalluste

24.04.2021

Annotatsioon

Lõputöö eesmärgiks on selgitada, kuidas toimib makse algatamise teenus, võrrelda seda erinevate kastuses olevate e-poe makselahendustega ning kirjeldada toimiva makse algatamise teenuse tööpõhimõtteid, ehitust ja süsteemi arhitektuuri.

Lõputöö relisatsioon põhineb ettevõttes Montonio Finance arendatud makse algatamise teenusel ning hõlmab kahte peamist komponenti milleks on REST-teenus ning klientrakendus.

Realisatsiooni tulemusel on loodud makse algatamise teenus, mis teenindab kaupmehi ning nende kliente üle 800 veebipoes ning millega sooritatakse keskmiselt 4000 makset päevas.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 23 leheküljel, 6 peatükki, 18 joonist, 2 tabelit.

Abstract

Development of a Payment Initiation Service Based on the European Payment Services Directive PSD2

The aim of this thesis is to explain how the payment initiation service works, compare it with the various online payment solutions avaliable, and describe the operating principles, development and system architecture of a functioning payment initiation service.

The realization of this thesis is based on the payment initiation service developed by Montonio Finance and includes two main components: the REST-service and the web-based user interface.

As a result, a payment initiation service has been developed that serves merchants and their customers in over 800 online stores and initiates an average of 4,000 transactions per day.

The thesis is in Estonian language and contains 23 pages of text, 6 chapters, 18 figures, 2 tables.

Lühendite ja mõistete sõnastik

PSD2	Teine makseteenuste direktiiv
API	*Application Programming Interface*, rakendustarkvara liides
REST	*Representational State Transfer*, veebiressurside liides
JWT	*Json Web Token*, krüptitud andmete edastusviis kahe osapoole vahel
OAuth	Metoodika kasutaja tuvastamiseks üldiste API-de ja tasuta juurutamise kaudu.
Klient	Rakenduse kasutaja, kes sooritab makse algatamise teenuse abil ostu e-poest
Kaupmees	Rakenduse kasutaja, kes kogub makse algatamise teenuse abil oma e-poes makseid
API Võti	Unikaalne tähe -ja numbrimärkide kombinatsioon, mille abil autenditakse päringuid
Klientrakendus	Rakendus, milles klient sooritab makse
Webhook	Viis teavituste saatmiseks tarkvaraliideste vahel
ASPSP	*Account servicing payment service provider,* pank
Salajane võti	Kaupmehe salajane võti REST-teenusega suhtlemiseks
Avalik võti	Kaupmehe avalik võti REST-teenusega suhtlemiseks
HTML	*HyperText Markup Language,* keel milles märgendatakse veebilehti
CSS	*Cascading Style Sheets,* keel veebilehtede kujundamiseks

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Tehnoloogia kiire areng ning kommunikatsiooni ja logistika paranemine on toonud endaga kaasa olulise nihke ka kaubandusmaastikul. Füüsilistest kauplustest liigutakse aina enam e-kaubanduse poole ning inimeste ostuharjumused ja mugavuskäitumine soosivad e-poodide kasvu. Kaupmeeste tähelepanu keskpunktiks on siinkohal saamas veebipoodi külastavate klientide mugavus, hüljatud ostukorvide hulga minimeerimine ning ostukorvi eest tasumiseks võimalikult turvaline, kiire ning usaldust tekitav lahendus.

14. septembril 2019 jõustus Euroopa Liidus teine makseteenuste direktiiv ehk PSD2, mis võimaldab turule tulla finantstehnoloogia ettevõtetel, pakkudes kaupmeestele ning klientidele senisest odavamaid ning mugavamaid finantslahendusi. Avatud pangandus võimaldab ettevõtetel arendada välja näiteks uut liiki makselahendusi milleks on makse algatamise teenus. Avatud Panganduse tuumaks on pankade avalikud REST-teenused, mis võimaldavad kolmanda osapoole litsentsitud teenusepakkujatel luua finantsrakendusi ja osutada finantsteenuseid. See tähendab, et pangad on kohustatud litsenseeritud ettevõtetele lubama liidestusi panga süsteemidega, mis kuni direktiivi jõustumiseni olid kinnised ning ainult panga siseseks kasutamiseks.

Lõputöö kirjeldab ettevõttes Montonio Finance loodud makse algatamise teenust ning selle realisatsiooni. Töö autor planeeris süsteemi arhitektuuri, osales REST-teenuse arendamisel ning arendas täielikult välja teenuse klientrakenduse. Töö peamised osad on klientrakendus, andmebaas ning REST-teenus, mis omakorda jaguneb kolmeks alamosaks: kaupmehe autentimine, kliendi autentimine ning makse algatamine.

2 Taust ja olemasolevad lahendused

Eesti e-kaubanduse maastikul on siiani kasutusel olnud kolm suuremat lahendust, mida kaupmehed oma klientidele pakuvad, et ostu eest e-poes turvaliselt tasuda – Maksekeskus, pangalingid ning kaardimaksed.

Lisaks eelnimetatutele esitavad üksikud kaupmehed veebipoest ostetud kauba eest tasumiseks kliendile arve. Välismaised maksete vahendamisele suunatud ettevõtteid nagu PayPal kohtab eesti veebipoodidest harva, kuna eesti kliendi makseharjumused ning soov näha oma kodupanka maksemeetodite hulgas ei ole siiani soosinud nende kasutuselevõttu.

14. septembril 2019 jõustus Euroopa Liidu liikmesriikides PSD2 ehk täiendatud makseteenuste direktiiv [1], mis võimaldab kolmandatel osapooltel osutada tarbijale pangaga seotud teenuseid. Avatud pangandus tähendab, et pangandusteenuseid nagu maksete algatamine või kontoinfo kuvamine saavad edaspidi lisaks pankadele pakkuda ka teised teenuseosutajad sealhulgas finantstehnoloogia ettevõtted ja maksevahendajad. Klientide jaoks tähendab see valikuvõimaluste laienemist läbi suurenenud teenusepakkujate vahelise konkurentsi. See on panganduse jaoks sama oluline samm nagu oli telefoninumbri mobiilsus telekommunikatsioonile või elektrituru avamine energiasektorile [16].

2.1 Kaardimaksed

Kaardimaksed on füüsilistes poodides enimlevinud viis ostu eest tasuda. Ka e-poodides võimaldavad enamus kaupmehi oma klientidel seda makseviisi kasutada. Ajalooliselt on oma krediitkaardi andmete sisestamine e-poodidesse olnud kliendi jaoks ebausaldust tekitav protsess, kuna veel mõnda aega tagasi oli võrdlemisi lihtne selliselt kaardipettusi toime panna. 2019. aasta Consumer Sentineli Networki andmetel oli krediitkaardi pettuste kohta aasta jooksul 271 823 teadet, mis tegi krediitkaardipettused 2019. aastal kõige sagedamini teatatud ID-pettuste tüübiks [22]. Uus turvasüsteem nimega 3D Secure 2 muudab informatsiooni voo kaupmeeste ning pankade vahel senisest kiiremaks ning

turvalisemaks kasutades täiendavat kliendi identifitseerimist, kuid sellegipoolest eelistatakse võimalusel kasutada veebipoodides mõnd muud makselahendust.

2.2 Pangalingid

Pangalingid kujutavad endast pankade endi poolt arendatud mooduleid, mille kaupmehe poolsel paigaldamisel e-poodi on kliendil võimalik tasuda ostu eest ühe panga kontolt selle sama panga kontole [2]. See tähendab, et kui kaupmees soovib võimaldada klientidel oma e-poes tasuda kolmest pangast, näiteks Swedbank, SEB, LHV, peab ta oma veebipoodi lisama kõigi nimetatud pankade moodulid ning avama nendes pankades arvelduskontod. Kuna eestis on viis laialt levinumat panka, kujuneb ükshaaval pankade liidestamine kaupmehele nii ajaliselt kui ka rahaliselt kulukaks, nõudes lisa arendustunde ning lepingu sõlmimist iga pangaga. Ka raamatupidamislikult on pangalinkide kasutamine raskendatud, kuna eri pankadest tehtud maksed jõuavad erinevatele pangakontodele ning mitme arvelduskonto paralleelne haldus suurendab raamatupidaja töömahtu.

2.3 Rahasiire

Rahasiire on makseteenus, mille käigus rahalised vahendid edastatakse maksjalt saajale või tema nimel tegutsevale makseteenuse pakkujale ilma raha maksja või saaja nimel maksekontot avamata [14].

Peamine eestis tegutsev makseteenuse pakkuja, kes oma tegevuse osutamiseks rahasiiret kasutab on AS Maksekeskus. Kuigi sisemiselt kasutab ka maksekeskus pangalinke, on ta kaupmehe jaoks oluliselt mugavam. Kaupmees sõlmib lepingu Maksekeskusega ning saab seejärel alla laadida Maksekeskuse mooduli mis sisaldab liidestusi kõikide pankadega [3]. Kliendi jaoks ei ole Maksekeskuse ja pangalinkide vahel suurt erinevust, kuna klient teeb ostu sooritamiseks siiski ühe ülekande, mis läheb maksekeskuse kontole. Seejärel kannab Maksekeskus raha regulaarselt kaupmehe kontole ning mõlema tehingu sooritamiseks kasutatakse pangalinke.

Kuna rahasiirde teenuse osutamiseks on seni olnud siiski vaja kasutada pangalinke, ning selleks, et raha jõuaks kliendi kontolt kaupmehe kontole, tehakse kokku kaks kannet, tõuseb selliselt teenuse osutamise maksumus kaupmehele, mis tihtipeale tähendab

kõrgemat toote hinda lõpptarbijale. Pangalinkide ning teiste maksemeetodite hinnastust on võrreldud ülejärgmises peatükis.

2.4 Makse algatamise teenus

Makse algatamise teenus on uue põlvkonna makselahendus. Avatud panganduse reeglite alusel saavad kliendid muu hulgas võimaluse pangale nõusoleku andmiseks oma andmete jagamiseks mittepangast teenusepakkujatele, kes saavad pakkuda klientidele uusi ja põnevaid teenuseid, näiteks ka maksete algatamist kliendi kontolt [16].

Uus direktiiv võimaldab esimest korda ajaloos tulla turule makseteenustel, mille kasutamisel annab klient makse algatamise teenuse pakkujale nõusoleku kanda kliendi kontolt määratud summa otse kaupmehe kontole kasutamata selleks pangalinke või hoidmata raha vahesammuna teenusepakkuja kontol. Pankade rakendusliideste kasutamine on teenusepakkujatele tasuta ning pangal ei ole õigust lisatasusid küsida. See tähendab, et e-poe maksete hinnastus on võimalik tänu uuele direktiivile tuua rekordiliselt madalale.

2.5 Makseteenuste hinnastus

Kliendilt maksete kogumine on tasuta vaid siis, kui klient tasub sularahas. See aga ei ole e-poes tehtud ostude puhul võimalik ning makselahenduse hind on üks olulisemaid tegureid, mida kaupmees jälgib endale sobivat teenusepakkujat valides. Tabelil 1 on välja toodud pangalinkide, Maksekeskuse ning loodud toote, Montonio makse algatamise teenuse hinnastused ühe tehingu kohta.

Teenusepakkuja	**Hind makse kohta**
SEB	1% (min 0,13 €)
Swedbank	1% (min 0,13 €, max 3,2 €)
Luminor	1% (min 0,13 €)
Luminori e-kaubanduse portaal	1,5% (min 0,15 €)
LHV	1% (max 3 €)
Coop	0,15 € + km

Maksekeskus	2,5% + 0,3 € + km
Montonio	0,05 € + km

Tabel 1. Teenusepakkujate hinnastused [15]

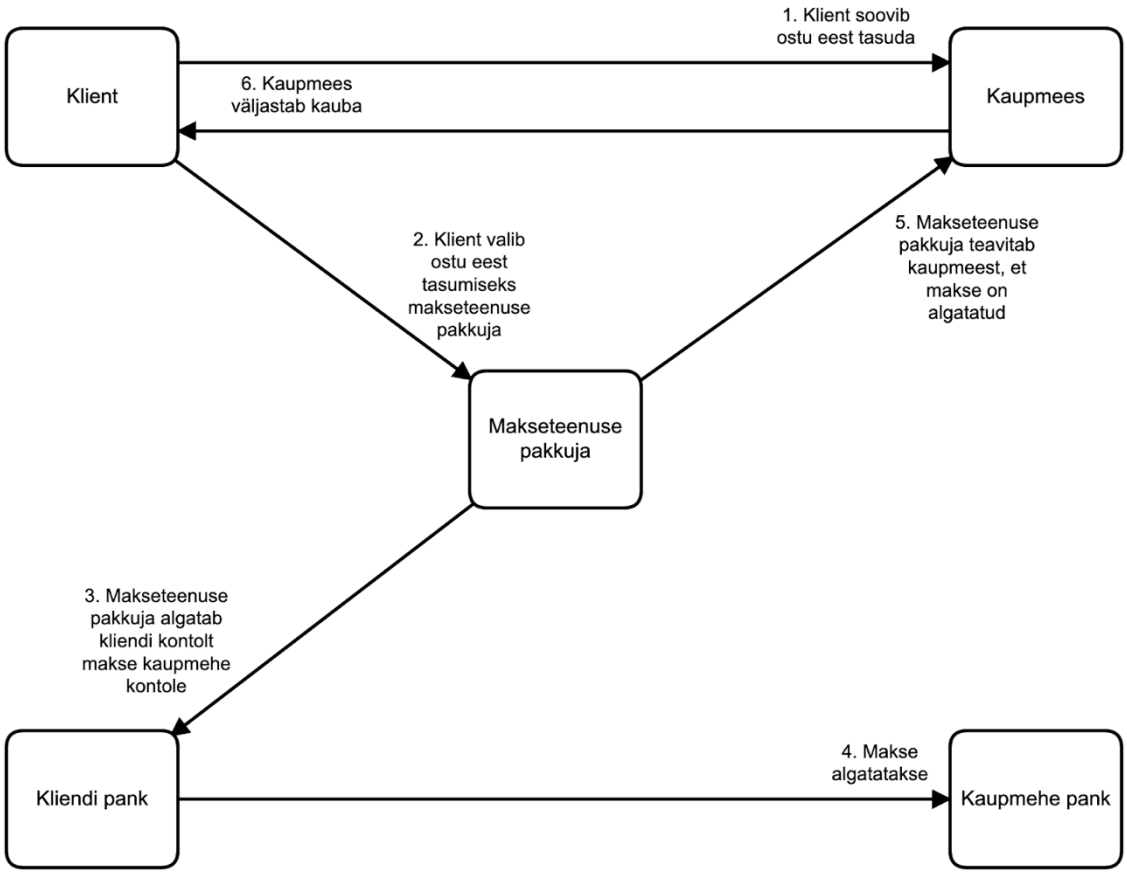
Enamus pankasid pakuvad makseteenust hinnastusega 1% tehingult ning miinimumtasu jääb vahemikku 0,13 € - 0,15 €. Swedbank ja LHV on määranud ka maksetehingult võetava teenustasu ülemise piiri vastavalt 3,2 ja 3 eurot.

Maksekeskuse teenustasud on aga pangalinkidest oluliselt kõrgemad, pürgides 2,5% makse summast mille otsa liidetakse fikseeritud tasu 0,3 €. Maksekeskuse kõrge teenustasu on põhjendatud kaupmehe mugavuse ning vähendatud liidestuste ja lepingute arvuga, mille kaupmees peaks pangalinkide puhul iga pangaga eraldi sõlmima. Nimetatud lahendustest on hetkel turul odavaim Montonio makselahendus, mis kasutab maksete teostamiseks makse algatamise teenust ning mille hinnastuseks on määratud 0,05 € tehingult.

3 Analüüs ja nõuded

Makse algatamise teenus koosneb kolmest suuremast komponendist milleks on REST-teenus, klientrakendus ning moodulid mille paigaldamisel e-poodi luuakse suhtlus makse algatamise teenuse pakkuja REST-teenuse ning e-poe vahel. Liidestamiseks vajalike moodulite arendus jääb lõputöö skoobist välja.

Selleks, et kaupmees saaks oma e-poes maksete kogumiseks kasutada makse algatamise teenust on tal vaja leida sobiv teenusepakkuja ning lisada oma veebipoele teenusepakkuja moodul. Järgnevalt on toodud joonis, mis kirjeldab, milline on makse algatamise teenuse üldtööpõhimõte ning millised sammud teeb süsteem selleks, et makse sooritada (Joonis 1).



Joonis 1. Makse protsess ning osaliste vaheline suhtlus

Protsessi algatab klient sooviga sooritada ost, valides ostukorvi eest tasumiseks makse teenuse pakkuja. Turu tava on, et e-poodi paigaldatavad moodulid tekitavad ostukorvi pankade logod nii, et klient valib juba ostukorvis panga millega soovib maksta ning alles seejärel suunatakse ta makseteenuse pakkuja vahelehele. Sellist kasutajavoogu kasutatakse, et suurendada kliendi turvatunnet, nähes oma kodupanka maksemeetodite hulgas ning vähendada seeläbi mahajäetud ostukorvide hulka. Pärast panga valimist algatab makse teenuse pakkuja makse kliendi kontolt kaupmehe kontole ning teavitab seejärel kaupmeest sooritatud maksest. Viimase sammuna väljastab kaupmees kauba.

3.1 Nõuded

REST-teenus peab olema ehitatud võimalikult modulaarselt, kuna iga pangaga, millega süsteem suhtleb tuleb luua eraldi liidestused ning need ei tohi teineteise tööd segada. Süsteemi piisav modulaarsus annab ühtlasi võimaluse liidestada tulevikus vähese vaevaga ning süsteemi ümber kirjutamata ka välisriikide panku, et laieneda üle Euroopa.

Süsteem peab olema turvaline ning jätma kõikidest autentimistest ning makse algatamistest andmebaasi jälje. Võib tekkida olukord, kus klient autendib end ühes pangas ning soovib seejärel panka vahetada. Sellised ideaal-kasutusjuhtudest kõrvalekalded peavad olema hästi käsitletud. Näiteks kui klient on makse juba kinnitanud ei tohi olla võimalik sama tellimuse kohta uut makset algatada. See tähendaks, et klient saadab kaupmehele kahekordse summa. Ka klientrakenduse veateated peavad olema kliendile selged ja arusaadavad, et vältida nimetatud olukordi.

Süsteem peab olema võimeline teavitama kaupmehe veebipoodi nii sooritatud, kui ka pooleli jäänud maksest pärast makse lõpetamist ka juhul, kui klient ei jõua tagasi e-poodi ning sulgeb oma veebilehtiseja kohe pärast pangas makse kinnitamist või poolelijätmist. Sooritatud ja pooleli jäetud maksete kinnitamise süsteem on makseteenuste juures üks olulisemaid komponente, kuna võib suuresti mõjutada kaupmehe töövoogu.

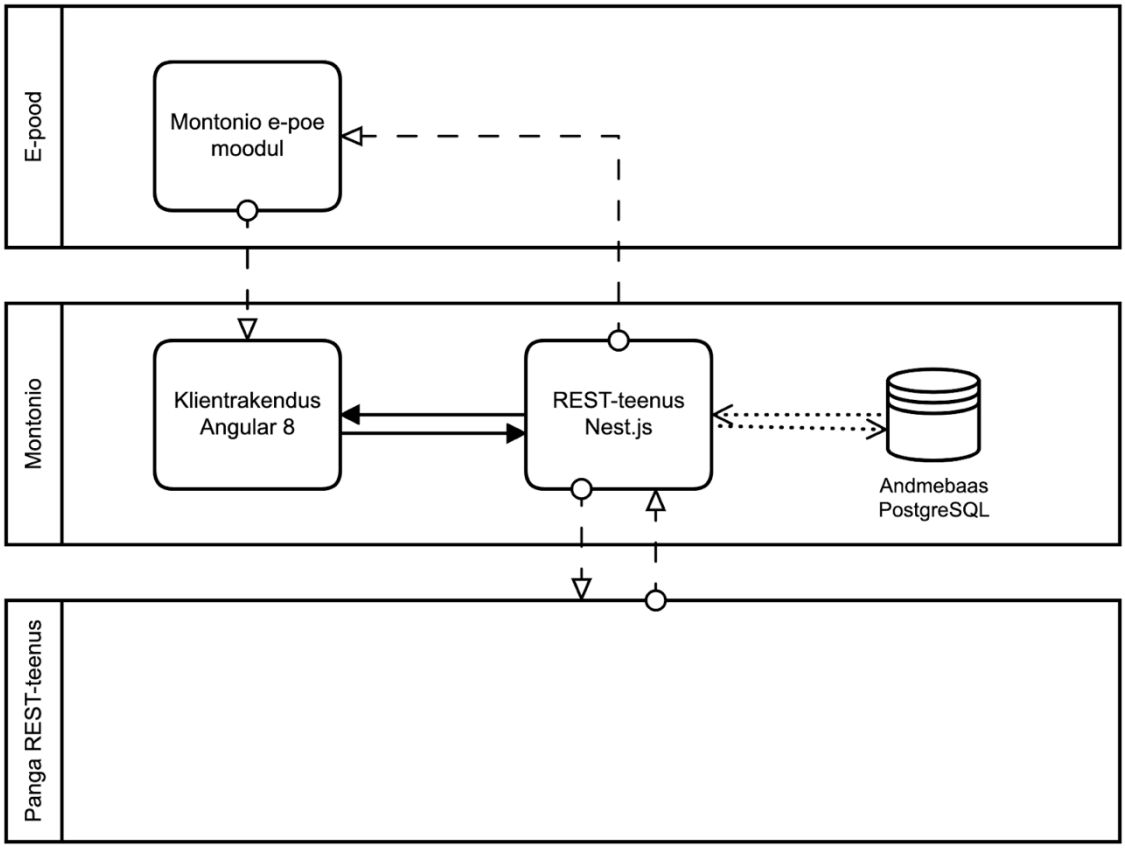
Klientrakendus peab toimima kõikides veebilehitsejates ja mobiilil veatult. Vältimaks halva või vigase rakenduse tõttu ostukorvi mahajätmist tuleb klientrakendust katsetada erinevatel seadmetel ning veebilehitsejates, et tagada parim võimalik töökindlus. Lisaks testimisele on klientrakendusele vajalik lisada ka monitoorimistarkvarad, mille abil tekkinud vigu kiirelt ja operatiivselt parandada.

4 Realisatsioon

Montonio makse algatamise teenuse tööks on vajalikud viis komponenti:

1. E-poe moodulid
2. Klientrakendus
3. REST-teenus
4. Andmebaas
5. Pankade REST-teenused

Järgneval joonisel on kirjeldatud komponentide vaheline suhtlus ning andmevoog (Joonis 2). Töö sisaldab endas Montonio siseste komponentide täpsemat analüüsi ning kirjeldust. E-poe moodulid ning pankade REST-teenused on välised komponendid, mida Montonio kasutab, et teenust osutada.



Joonis 2. Teenuse üldarhitektuur

4.1 REST-teenuse arhitektuur

Montonio REST-teenus on arendatud kasutades Nest.js raamistikku. Nest on aastal 2018 välja tulnud avatud lähtekoodiga raamistik, mis on tugevalt inspireeritud klientrakenduste arendamiseks mõeldud raamistiku, Angulari [6] struktuurist ja ülesehitusest [4]. Kuna makse algatamise teenuse klientrakendus ning varasemad teenused on arendatud Angularis, tundus loogiline võtta kasutusele Nest.js, et kulutada võimalikult vähe aega uue raamistiku tundmaõppimisele ning kirjutada algusest peale võimalikult kvaliteetset koodi.

Teenuse peamised alamkomponendid on kaupmehe autentimine, kliendi autentimine ning makse algatamine.

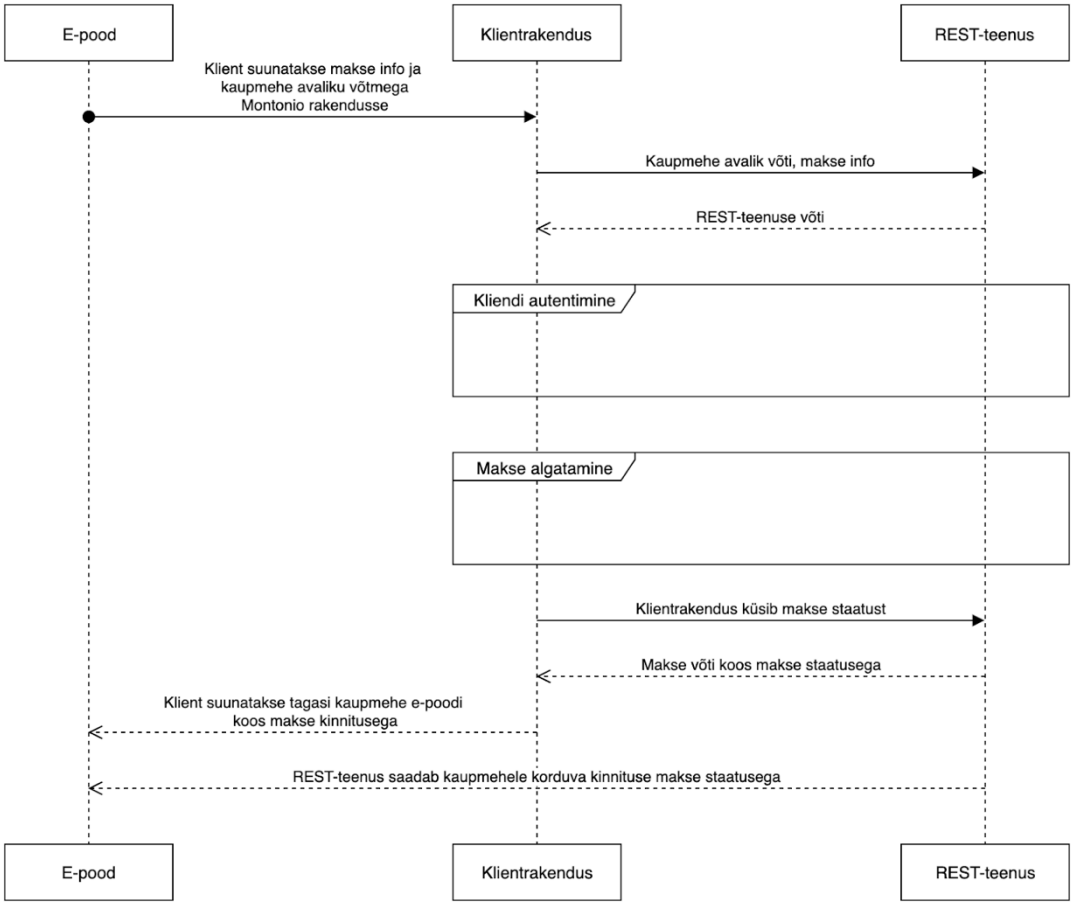
4.1.1 Kaupmehe autentimine ning „tunne oma klienti" põhimõte

Iga finantsteenuse pakkuja peab enne teenuse osutamist saama vastava loa regulaatorilt. Eestis on selleks Finantsinspektsioon, kellelt on võimalik taodelda luba ning kes ühtlasi peab volitatud ettevõtete üle järelvalvet [13].

Finantsinspektsioon kui finantsjärelevalveasutus on puutumuses rahapesu tõkestamisega eelkõige oma järelevalve alla kuuluvate finantsvahendajate kontrollimisel. Finantsinspektsiooni ülesanne on kontrollida, et pankade ja teiste finantsvahendajate organisatsioon ja riskijuhtimine oleks selliste protsesside ning süsteemidega, mis vastavad äristrateegiale ja riskiisule, ning oleks piisavalt mehitatud. See hõlmab nii krediidi andmist, makseteenuste ja investeerimisteenuste osutamist, kindlustusriske kui ka finantsvahendaja organisatsiooni laiemalt. „Tunne oma klienti" põhimõte moodustab osakese riskijuhtimisest ja selle põhimõtte täitmine kujutab endast tõket rahapesule [18].

Tulenevalt rahapesu tõkestamise kohustusest, on oluline, et Montonio kontrolliks oma makse algatamise teenust kasutavate ettevõtete tausta ning oleks veendunud müüdavate toodete legaalsuses. Seetõttu peab iga algatatud makse olema autenditud ning ühtlasi peab olema tagatud, et makse on algatatud kaupmehelt, kes on Montonio teenuse kasutamiseks heakskiidu saanud. Selleks kasutatakse kaupmeestele genereeritud unikaalseid võtmeid, millega kindlaks teha e-pood, kust makset algatada soovitakse.

Järgneval joonisel on välja toodud E-poe, Klientrakenduse ning REST-teenuse vaheline suhtlus ja kaupmehe poolse makse algatamise autentimine (Joonis 3).



Joonis 3. Kaupmehe autentimine

Esimese sammuna allkirjastab kaupmees oma e-poes makse info oma Montonio poolt genereeritud salajase võtmega ning suunab seejärel kliendi Montonio kasutajaliidesesse. Allkirjastatud makse info antakse kaasa ümbersuunamise lingi parameetrina.

Allkirjastatud võtme sisus on kohustuslikud parameetrid:

1. Summa
2. Valuuta
3. Kaupmehe avalik võti
4. Kaupmehe tellimuse ID
5. Makse aegumise ajamärk
6. Link millele klient suunatakse pärast õnnestunud makset

Lisaks eelmainitutele on võimalik võtme sisule lisada:

1. Kaupmehe nimi
2. Link mille kaudu kaupmehele saata kaupmehele lisateavitus pärast makse lõpetamist
3. Makse selgitus
4. Viitenumber
5. Teenuse keel
6. Kliendi andmed

Järgenvalt on toodud näide võtme genereerimisest ning võtme sisust (Joonis 4). Võti on JWT kujul ning sisaldab andmeid JSON formaadis. Võtme allkirjastab kaupmees oma e-poes salajase võtmega mille on Montonio süsteem talle väljastanud, et tagada andmete terviklus. Andmete terviklus tähendab, et andmed peavad olema usaldusväärsed ja autentsed ning volitamata muudatused peavad olema tuvastatavad ja kõrvaldatavad [17].

```
const jwt = require('jsonwebtoken');

const payload = {
    amount: 10,
    currency: 'EUR',
    access_key: 'merchant_access_key',
    merchant_reference: 'SO661123',
    merchant_return_url: 'https://montonio.com/orders/27731773/thank_you',
    merchant_notification_url: 'https://montonio.com/orders/payment_webhook',
    payment_information_unstructured: 'Payment for order SO661123',
    preselected_aspsp: 'LHVBEE22',
    preselected_locale: 'et',
    checkout_email: 'test-customer@montonio.com'
}

const token = jwt.sign(
    payload,
    secretOrPrivateKey: 'merchant_secret_key',
    options: {algorithm: 'HS256', expiresIn: '10m'}
);
```

Joonis 4. Makse andmete allkirjastamine

Pärast võtme genereerimist ning kliendi sellega Montonio klientrakendusse suunamist saadab klientrakendus võtme REST-teenusele, kus see dekodeeritakse ning võrreldakse võtme kehas olevat kaupmehe avalikku võtit andmebaasis oleva kaupmehe avaliku võtmega. Kui need klapivad, saab Montonio kindel olla, et päring tuli Montonio partnerilt ning võtmes oleva makse info põhjal luuakse süsteemi uus makse. Klientrakendusele saadetakse tagasi uus genereeritud võti, millega autenditakse edasised päringud REST-teenuse ning klientrakenduse vahel.

4.1.2 Kliendi autentimine, OAuth

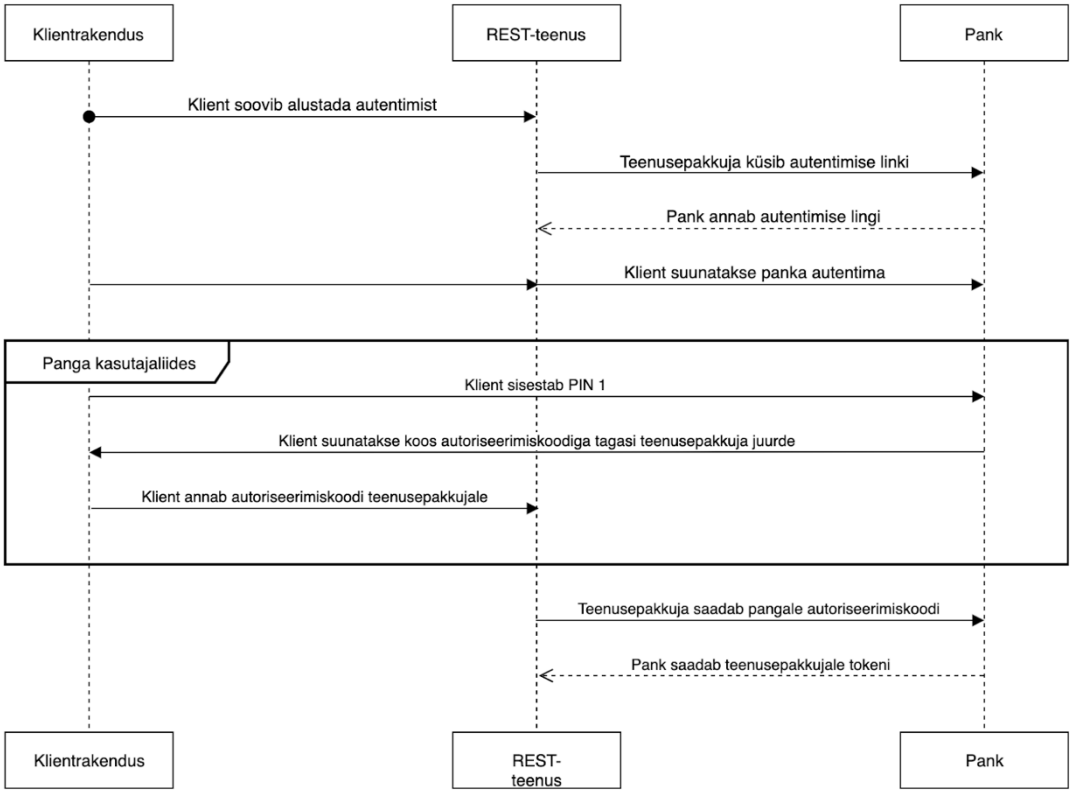
Kliendi autentimine on maksete turvalisuse tagamiseks üks kõige olulisemaid samme. Makse algatamise teenuses on kasutusel ümbersuunamise põhimõttel toimiv autentimine.

Autentimise protsess algab kliendi soovist end autentida Montonio klientrakenduses mille peale REST-teenus küsib pangalt autentimise linki. Seejärel saadab pank makse teenuse pakkujale autentimise lingi ning klient suunatakse panga lehele end autentima. Sellist autentimisviisi nimetatakse OAuth [5] tehnoloogiaks, milles kliendi või kasutaja autentimiseks kasutatakse kolmandat usaldatud osapoolt. Makse algatamise teenuse puhul on kolmandaks osapooleks pank, millest klient soovib makset algatada.

Pärast kliendi õnnestunud autentimist suunatakse ta tagasi makse teenuse pakkuja klientrakendusse koos autoriseerimiskoodiga, mis omakorda saadetakse klientrakendusest REST-teenusele.

REST-teenus küsib seejärel pangalt API võtit, saates päringuga kaasa saadud autoriseerimiskoodi. Kui pank tuvastab, et autoriseerimiskood on kehtiv, saadab ta REST-teenusele tagasi API võtme millega teha edasisi päringuid makse teenuse pakkuja rakendusliidese ning panga vahel (Joonis 5).

Iga kliendi poolt alustatud autentimise peale Montonio kasutajaliideses tekitatakse andmebaasi uus rida. Pärast õnnestunud autentimist uuendatakse real olevat staatuse veergu. Selliselt kõiki samme registreerides on võimalik kiiresti aru saada, kas mõne panga autentimisteenuses esineb mingil ajahetkel tõrkeid ning sellest tulenevalt pangale tagasisidet anda, kuidas oma autentimisteenust parandada.



Joonis 5. Kliendi autentimine, OAuth

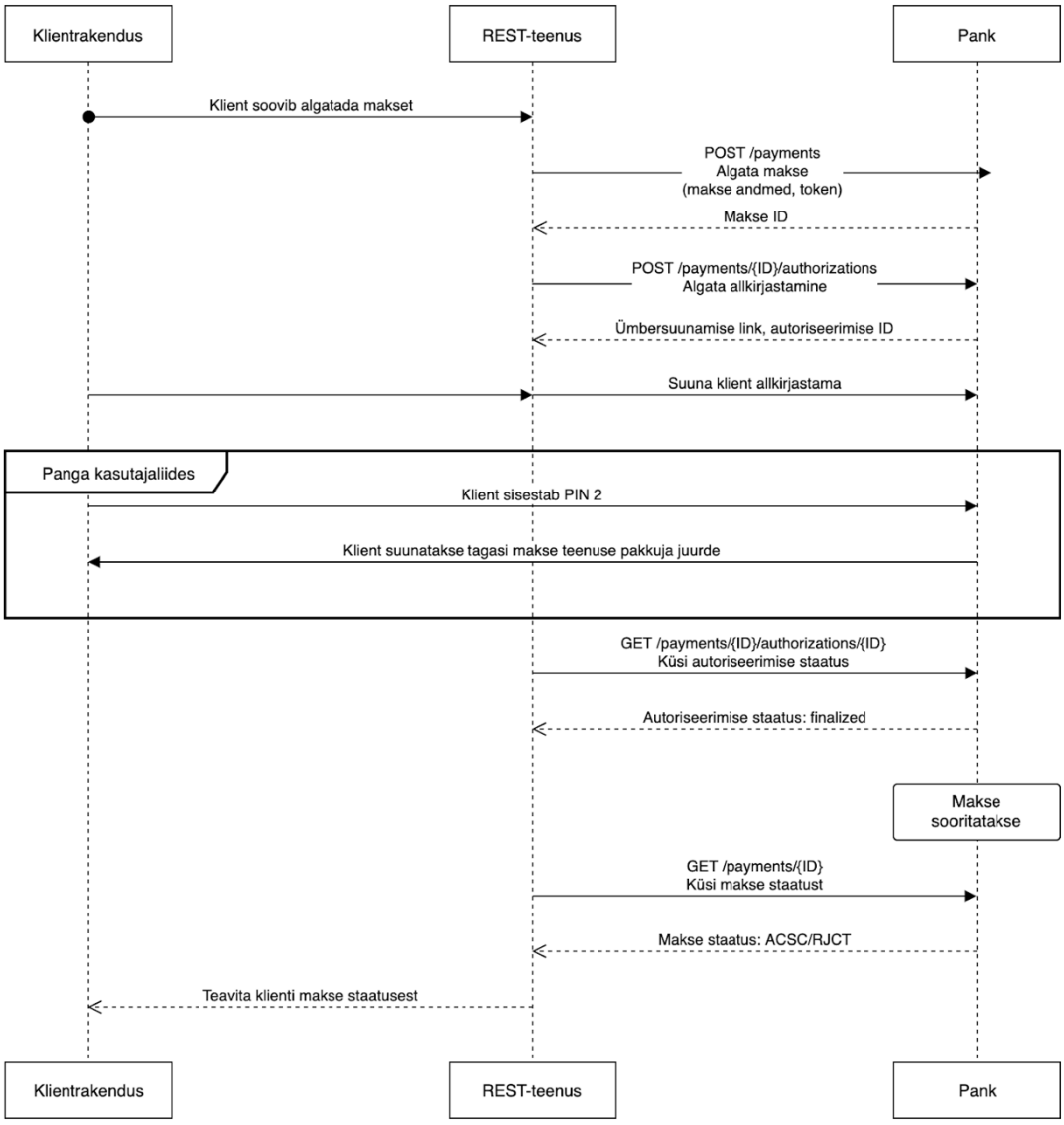
4.1.3 Makse algatamine

Kui klient on pangas end autentinud ning makse teenuse pakkuja REST-teenus on pangalt saanud võtme, algab makse algatamise protsess.

Esimese sammuna annab klientrakendus REST-teenusele teada soovist makse kliendi nimel algatada. Pangalt saadakse ümbersuunamise link ning klient suunatakse lingile, et makse kinnitada. Pärast kliendi tagasisuunamist makse teenuse pakkuja klientrakendusse küsitakse pangalt makse staatus ning õnnestunud makse puhul suunatakse klient tagasi kaupmehe juurde.

Makse algatamine on andmebaasi tasemel alati seotud ühe autentimisega. Kui klient on juba makse algatanud, kuid otsustab panka vahetada suunatakse ta tagasi panga valikusse, kust on võimalik uuesti end mõnes teises pangas autentida. Andmebaasi tekitatakse seega uus autentimise kirje, ning seotakse see maksega. Eelmised autentimised määratakse tühistatuks.

Täpsem päringute selgitus ning voog on leitav järnevalt jadadiagrammilt (Joonis 6), mis kirjeldab igat päringut, mis makse teenuse pakkuja ning panga vahel tehakse.



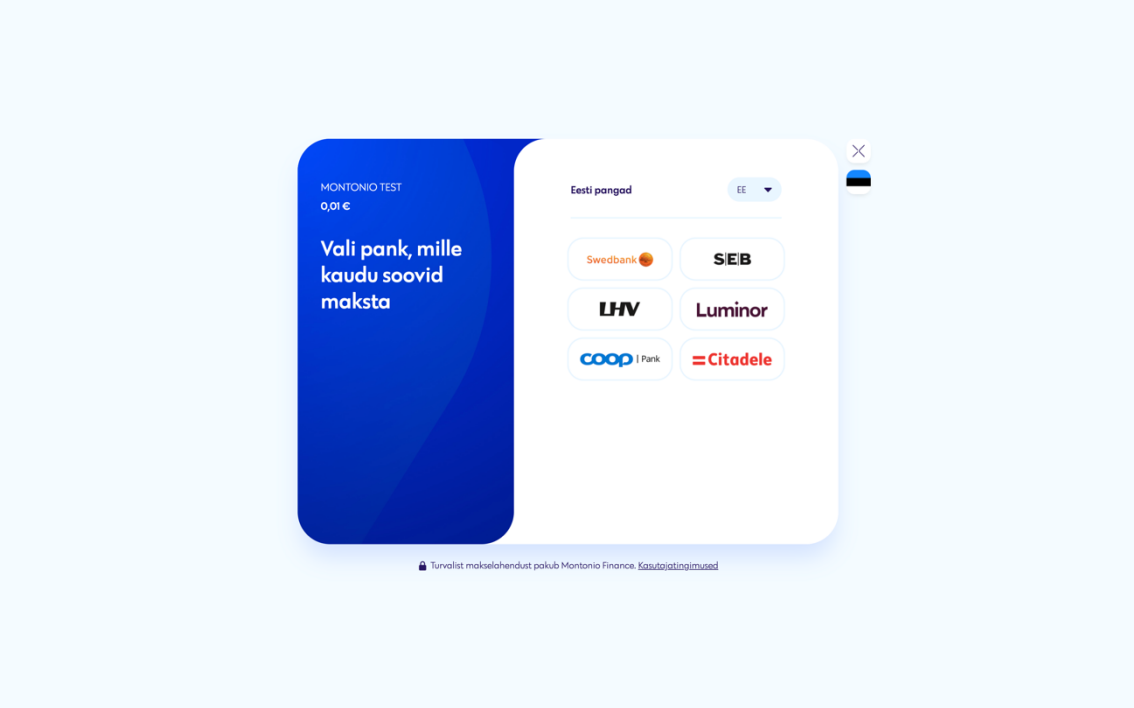
Joonis 6. Makse algatamine

4.2 Klientrakenduse arhitektuur

Montonio klientrakendus on arendatud kasutades raamistikku Angular 8. Angular on valitud, kuna ka teised tooted ning ettevõtte siseseks kasutamiseks mõeldud rakendused on arendatud Angularis. Arendamine nimetatud raamistikuga on kiire ning võrdlemisi lihtne, kuna annab näiteks võrreldes teise populaarse raamistiku Reactiga ette hulganisti tööriistu ning üsna kindlaks määratud tavad, mida järgides on lihtne ka teistel arendajatel süsteemist hõlpsasti aru saada [6].

Klientrakenduse peamine eesmärk on olla vaheaknaks panga ning Montonio REST-teenuse vahel. Näiteks pärast autentimist suunab pank kliendi teenusepakkuja valitud lingile koos autoriseerimiskoodiga. Et see toiming oleks kliendile visuaalselt ilus ning piisavalt ennast selgitav, on Montonio loonud mugava ning värske väljanägemisega klientrakenduse.

Kliendi jaoks algab kasutajateekond makse teenuse pakkuja valikust kaupmehe ostukorvis, misjärel suunatakse ta teenusepakkuja vahelele, kus tuleb valida pank, millega ostu eest tasuda. Kui kaupmees oma e-poodi pankade logosid ei lisa, on kliendil võimalik makse sooritamiseks sobiv pank valida klientrakenduse esimeses vaates (Joonis 7).



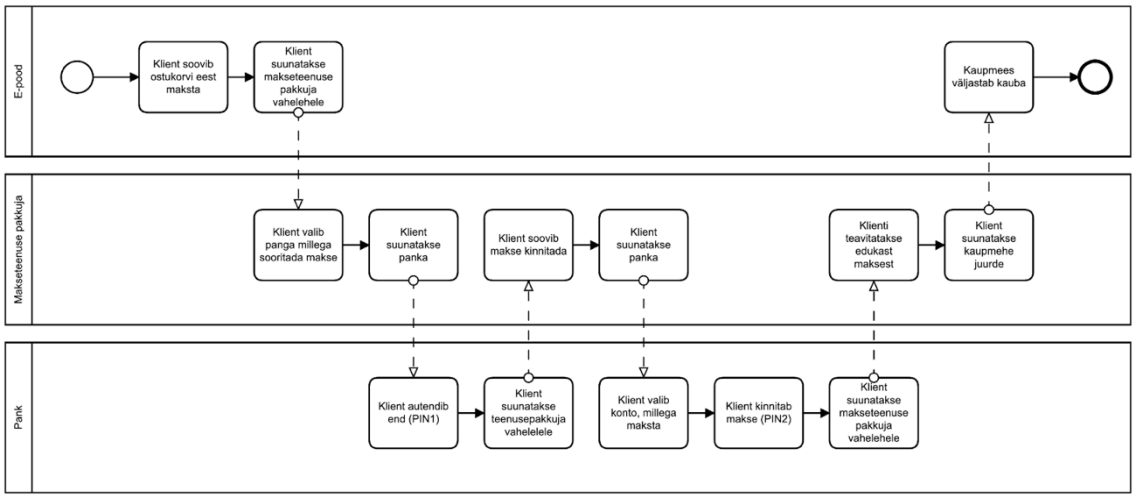
Joonis 7. Kasutajaliides: panga valik

Pärast panga valikut suunatakse klient panka end autentima (Joonis 15). Olles end edukalt autentinud (Joonis 16), suunatakse klient tagasi Montonio klientrakendusse koos auteriseerimiskoodiga, mille peale REST-teenus pärib pangalt makse kinnitamise linki ning klient suunatakse uuesti panka, nüüd juba makset kinnitama (Joonis 17). Pärast makse edukat kinnitamist (Joonis 18) suunab pank kliendi Montonio klientrakendusse, kus klienti teavitatakse sooritatud ostust (Joonis 8) ning pärast väikest ooteaega suunatakse automaatselt tagasi e-poodi, mis ühtlasi toimib kaupmehele teavitusena sooritatud maksest.

Joonis 8. Kasutajaliides: õnnestunud makse

Kui klient mingil põhjusel pärast pangas makse kinnitamist veebilehitseja sulgeb, ei suunata teda tagasi Montonio vahelele, mis omakorda tähendab, et kaupmeest ei teavitata makse lõppstaatusest. Selle probleemi lahendamiseks kasutab montonio *webhook*'e, mis tähendab, et kindla aja möödudes saadetakse kaupmehe veebipoele HTTP päringuga teavitus makse staatusest. Klientrakenduse vaated on leitavad Lisas 1.

Järgnevalt on kirjeldatud e-poes, Montonio klientrakenduses ning pangas toimuv kliendi kasutajateekond (Joonis 9).



Joonis 9. Kliendi kasutajateekond

Kasutajaliidese töökindluse tagamiseks monitooritakse rakendust kolmandate osapoolte tarkvaradega milleks on Sentry ning LogRocket. Sentry on tarkvara, mis püüab kinni kõik kasutajaliides tekkivad veateated ning edastab need Sentry konsooli, kus on võimalik vigu analüüsida ning selle põhjal klientrakenduses muudatusi teha. Sentry integratsioon on tehtud väga lihtsaks ning toetab üle 30 programmeerimiskeele [19].
Järgnevalt on toodud näide Sentry integreerimisest (Joonis 10).

```
Sentry.init({
    dsn: "https://examplePublicKey@o0.ingest.sentry.io/0",

    // Alternatively, use `process.env.npm_package_version` for a dynamic release version
    // if your build tool supports it.
    release: "my-project-name@2.3.12",
    integrations: [new Integrations.BrowserTracing()],

    // Set tracesSampleRate to 1.0 to capture 100%
    // of transactions for performance monitoring.
    // We recommend adjusting this value in production
    tracesSampleRate: 1.0,

});
```

Joonis 10. Sentry integratsioon [20]

LogRocket on tarkvara, mis võimaldab salvestada kasutaja liikumist rakenduses, muutes võimalikuks kasutajateekondade ning kasutajamugavuse analüüsi võttes arvesse reaalsete klientide käitumist. LogRocket ei salvesta kasutajateekonda video formaadis, vaid rekonstrueerib klientrakenduse vaated veebilehitsejas leitava CSSi ning HTMLi põhjal ning salvestab vaid kasutaja kursori liikumise. Lisaks kasutajamugavuse analüüsimisele annab LogRocketi kasutamine võimaluse teada saada ka vigadest, mis Sentrysse ei jõudnud, kuna LogRocket konsoolis on võimalik näha kõiki REST-teenusele tehtud päringuid ning nende vastuseid. Sentry ning LogRocket on võimalik omavahel ühendada nii, et iga Sentrysse jõudnud veateade on seotud vastava salvestusega LogRocketis. Selliselt mitme monitoorimistarkvara kasutamine annab hea ülevaate ning mitmeid võimalusi vigade tuvastamiseks ja kiireks parandamiseks. Sensitiivne kasutajainfo on salvestustest peidetud, ning LogRocketi andmebaasi seda ei saadeta.
Järgnevalt on toodud näide LogRocketi integreerimisest klientrakendusega (Joonis 11).

```
LogRocket.init(YOUR_APP_ID, options: {
    network: {
        isEnabled: true,
    },
});
```

Joonis 11. LogRocketi integratsioon [21]

4.3 Andmebaasi arhitektuur

Rakenduse andmebaas on arendatud kasutades populaarset, avatud lähtekoodiga andmebaasisüsteemi PostgreSQL [7]. Andmebaasisüsteemi kavandades kaaluti ka võti-väärtus loogikal põhinevaid andmebaase nagu näiteks Amazon DynamoDB [8], kuid kiiresti sai selgeks, et võimalus tabelite vahelisi seoseid luua on makselahenduse töös vajalik ning relatsiooniline andmebaas on selle jaoks parim tööriist. Mugavamaks suhtluseks REST-teenuse ning andmebaasi vahel kasutatakse objekt-relatsioonvastenduse vahendit Sequelize [9] ning Sequelize-typescript [10].

4.3.1 Objekt-relatsioonvastendus

Objekt-relatsioonvastenduse tööriistad, lühendatult ORM, võimaldavad andmebaasiga suhtlemiseks kasutada SQL päringukeele asemel objektorienteeritud programmeerimisele lähedasemat süntaksit. ORM toimib SQL keele abstraktsioonina ning vähendab tihtipeale kirjutatud koodi mahtu [11]. Järgnevalt on toodud näide samast lausest nii SQL päringukeeles (Joonis 13) kui ka kasutades Sequelize relatsioonvastendust (Joonis 12).

```
const user = await this.userModel.findByPk(uuid, options: {
    attributes: ['uuid', 'first_name'],
    include: [
        {
            model: Business,
            attributes: ['uuid', 'legal_name'],
            include: [
                {
                    attributes: ['uuid', 'name'],
                    model: Store,
                },
            ],
        },
    ],
    logging: true
});
```

Joonis 12. Sequelize näidispäring

```
SELECT "User"."uuid",
       "User"."first_name",
       "businesses"."uuid"                       AS "businesses.uuid",
       "businesses"."legal_name"                 AS "businesses.legal_name",
       "businesses->UserBusiness"."uuid"         AS "businesses.UserBusiness.uuid",
       "businesses->UserBusiness"."user_uuid"    AS "businesses.UserBusiness.user_uuid",
       "businesses->UserBusiness"."role"         AS "businesses.UserBusiness.role",
       "businesses->UserBusiness"."business_uuid" AS "businesses.UserBusiness.business_uuid",
       "businesses->UserBusiness"."created_at"   AS "businesses.UserBusiness.createdAt",
       "businesses->UserBusiness"."updated_at"   AS "businesses.UserBusiness.updatedAt",
       "businesses->UserBusiness"."deleted_at"   AS "businesses.UserBusiness.deletedAt",
       "businesses->stores"."uuid"               AS "businesses.stores.uuid",
       "businesses->stores"."name"               AS "businesses.stores.name"
FROM "users" AS "User"
        LEFT OUTER JOIN ( "users_businesses" AS "businesses->UserBusiness" INNER JOIN "businesses" ON
        "businesses"."uuid" = "businesses->UserBusiness"."business_uuid" AND
        ("businesses->UserBusiness"."deleted_at" IS NULL)) ON "User"."uuid" = "businesses->UserBusiness"."user_uuid" AND
                                                              ("businesses"."deleted_at" IS NULL)
        LEFT OUTER JOIN "stores" AS "businesses->stores"
                        ON "businesses"."uuid" = "businesses->stores"."business_uuid" AND
                           ("businesses->stores"."deleted_at" IS NULL)
WHERE ("User"."deleted_at" IS NULL AND "User"."uuid" = 'ce5ed4d5-eb74-434f-b43e-b7fd19cdf555')
```

Joonis 13. SQL näidispäring

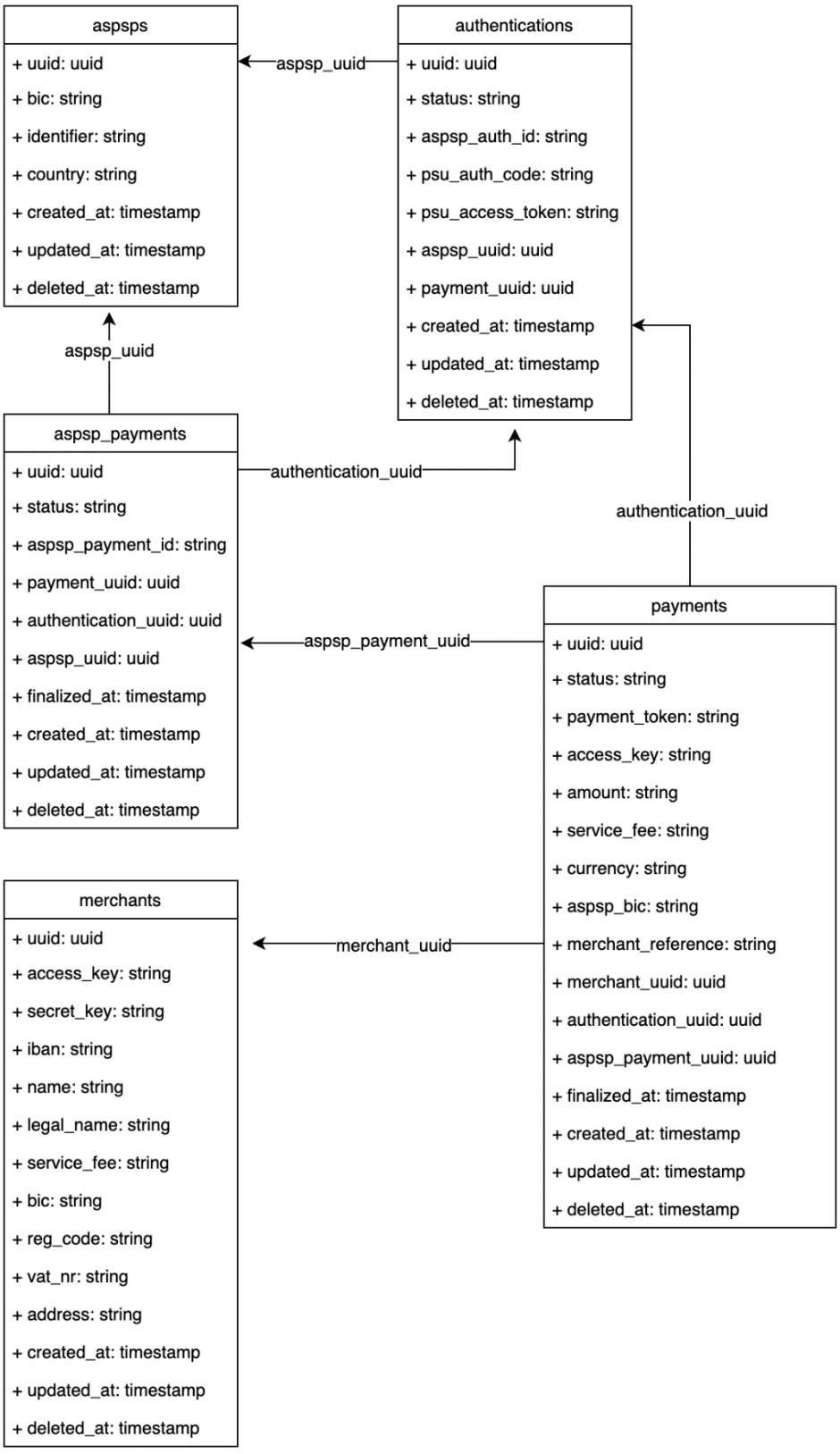
4.3.2 Andmebaasi tabelid

Makselahenduse andmebaas koosneb viies peamisest tabelist milleks on

1. aspsps
2. authentications
3. payments
4. aspsp_payments
5. merchants

Iga makse kohta tekitatakse andmebaasi tabelisse *payments* uus makse, kuhu on salvestatud kogu makse info. Kliendi autentimised on seotud tabeliga *authentications* ning iga makse allkirjastamise kohta ilmub rida tabelisse *aspsp_payments.* Kuna klient võib nii autentimise kui ka makse kinnitamise pangas tühistada, et valida ostukorvi eest tasumiseks mõni teine pank, võib iga *payments* tabelis oleva reaga seotud olla üks või rohkem *aspsp_payments* ning *authentications* tabelis olevat rida. Kaupmehe verifitseerimine toimub tabeli *merchants* abil, kus on kirjas kaupmehe info ning tema avalik ja salajane võti.

Järgneval joonisel on toodud tabelite lihtsustatud kirjeldus (Joonis 14). Veerge on pea igas tabelis tegelikult rohkem, kuid joonisel on kirjeldatud vaid makselahenduse tööks vajalikud andmed. Joonisel puuduolevad veerud on vajalikud rahapesu tõkestamise, turvalisuse ning monitoorimise eesmärkidel.



Joonis 14. Andmebaasi relatsiooniline mudel

5 Tulemused

Realisatsiooni tulemusel loodud süsteem võimaldab kaupmeestel makseid koguda kõikidest Eestis enimlevinud pankadest, mille hulgas on Swedbank, SEB, LHV, Luminor ning Coop Pank. Lisaks Eesti pankadele on süsteemiga integreeritud teisi Baltikumis kasutatavaid panku milleks on Citadele banka, Medicinos bankas, Šiaulių bankas ning OP pank. Lahenduse kasutamiseks tuleb kaupmehel oma veebipoodi lisada Montonio maksemoodul, mis võimaldab alustada maksete kogumist läbi makse algatamise teenuse.

Teenust kasutab töö kirjutamise hetkel üle 800 kaupmehe ning keskmiselt sooritatakse 4000 makset päevas. Kuna PSD2 ning pankade avalikud REST-teenused on võrdlemisi noored teenused, toimub Montonio ning pankade vahel tihe infovahetus ning tagasiside, kuidas teenuse kvaliteeti veelgi parandada.

5.1 Testimine

Süsteemi testimise automatiseerimine on suure külastatavusega teenuste töökindluse tagamise üks peamisi alustalasid. Montonio makselahenduse REST-teenusele on kirjutatud peamiselt E2E teste, mis on mõeldud süsteemi, kui terviku testimiseks. E2E testides ei kontrollita ühe kindla funktsiooni toimist, vaid süsteemile tehakse automatiseetritud päringuid, mille vastuseid kontrollitakse [12]. Kuna Montonio makselahenduse arhitektuuris esineb väga vähe iseseisvaid keerukaid funktsioone, mille testimiseks peaks kasutama Unit-teste, ning piisav E2E testimine kontrollib kaudselt pea kõikide funktsioonide tööd, kasutades selleks hulgaliselt teisi funktsioone ning loogikat, tundus selline lähenemine kõige praktilisem.

Järgnevalt on toodud tabel, mis annab ülevaate testide katvusest peamistel moodulitel (Tabel 2).

Moodul	**Moodul, %**	**Meetod, %**	**Rida, %**
payments	100%	78.13%	78.02%
authentications	100%	87.5%	73.86%
aspsp-payments	100%	80%	69.79%
merchants	100%	75%	70.79%
aspsps	100%	80%	69.79%

Tabel 2. Testide kattuvus peamistel teenusmoodulitel

6 Kokkuvõte

Lõputöö eesmärgiks oli luua makselahendus, mis kasutab tänu avatud panganduse direktiivile PSD2 võimalikuks saanud makse algatamise teenust. Teenus on arendatud ettevõttes Montonio Finance ning lõputöö autor osales süsteemi arhitektuuri planeerimises, REST-teenuse ülesehitamisel ning arendas välja veebilehitsejas toimiva klientrakenduse.

Süsteem on arendatud pidades silmas vajadust tulevikus liidestada lisaks Baltikumi pankadele hulgaliselt ka teisi Euroopas enimkasutatavaid panku ja laieneda lähitulevikus Poola, Hispaaniasse ning Saksamaale.

Avatud panganduse ning pankade avalike REST-teenuste arenemisel on plaanis teenusele lisada ka uusi funktsionaalsusi nagu näiteks perioodilised maksed ning mugav liides maksete tagastamiseks lõpptarbijale. Lisaks Montonio makselahenduse ning lisavõimaluste arendustele ettevõtte siseselt on oodata pankade REST-teenuste edasiarendusi. Näiteks massmaksete võimekuse väljaarendamine pankade poolt annab teenusepakkujatele võimaluse sooritada suurel hulgal makseid ühe allkirjastamisega, mis kiirendab kaupmeeste tööd näiteks tagastuste tegemisel. Lisaks eelmainitule on pankade arendusplaanis võimaldada makse algatamise teenuse läbi sooritada ka perioodilisi makseid, mis avab maksevahendajatele täiesti uue sektori ning võimaluse oma toodet veelgi laiahaardelisemaks muuta.

Montonio makse algatamise teenust täiendatakse igapäevaselt ja süsteemi töökindlus ning stabiilsus on kiiresti jõudnud järgi kaua turul valitsenud pangalinkidele. Uudse makse algatamise teenuse madal hinnastus ning väike mahajäetud ostukorvide on saanud kaupmeeste ning klientide sooja vastuvõtu, mis rajab jõudsalt teed muutuval e-kaubanduse maastikul.

Kasutatud kirjandus

[1] Pocopay: Avatud pangandus (PSD2). [WWW] https://pocopay.com/avatud-pangandus/ (18.04.2021)

[2] LHV: Pangalink. [WWW] https://www.lhv.ee/et/lhv-pangalink

[3] Maksekeskus: Pangalink.[WWW] https://maksekeskus.ee/service/pangalink/

[4] Medium: Nest 5: The official release Node.js in 2018. [WWW] https://medium.com/@kammysliwiec/nest-5-the-official-release-node-js-in-2018-1b6d3a47b104

[5] CSO: What is OAuth? How the open authorization framework works. [WWW] https://www.csoonline.com/article/3216404/what-is-oauth-how-the-open-authorization-framework-works.html

[6] Angular: The modern web developer's platform. [WWW] https://angular.io/

[7] PostgreSQL: The World's Most Advanced Open Source Relational Database. [WWW] https://www.postgresql.org/

[8] Amazon: Amazon DynamoDB. [WWW] https://aws.amazon.com/dynamodb/

[9] Sequelize: Sequelize ORM. [WWW] https://sequelize.org/#:~:text=Sequelize%20is%20a%20promise%2Dbased,loading%2C%20read%20replication%20and%20more.

[10] Robin Buschmann: Sequelize-typescript. [WWW] https://github.com/RobinBuschmann/sequelize-typescript

[11] Brian Cline: What is ORM. [WWW] https://www.brcline.com/blog/what-is-orm

[12] Guru99: What is E2E Testing with Example. [WWW] https://www.guru99.com/end-to-end-testing.html

[13] Finantsinspektsioon: Makse- ja e-raha teenused. [WWW] https://www.fi.ee/et/makse-ja-e-raha-teenused

[14] Eesti pank: Rahasiire. [WWW] https://www.eestipank.ee/rahasiire (20.02.2021)

[15] Veebikoda: E-poe pangalinkide tehingutasud. [WWW] https://veebikoda.com/eesti-pangalingid-hinnad/#maksekeskuse-alternatiiv (20.02.2021)

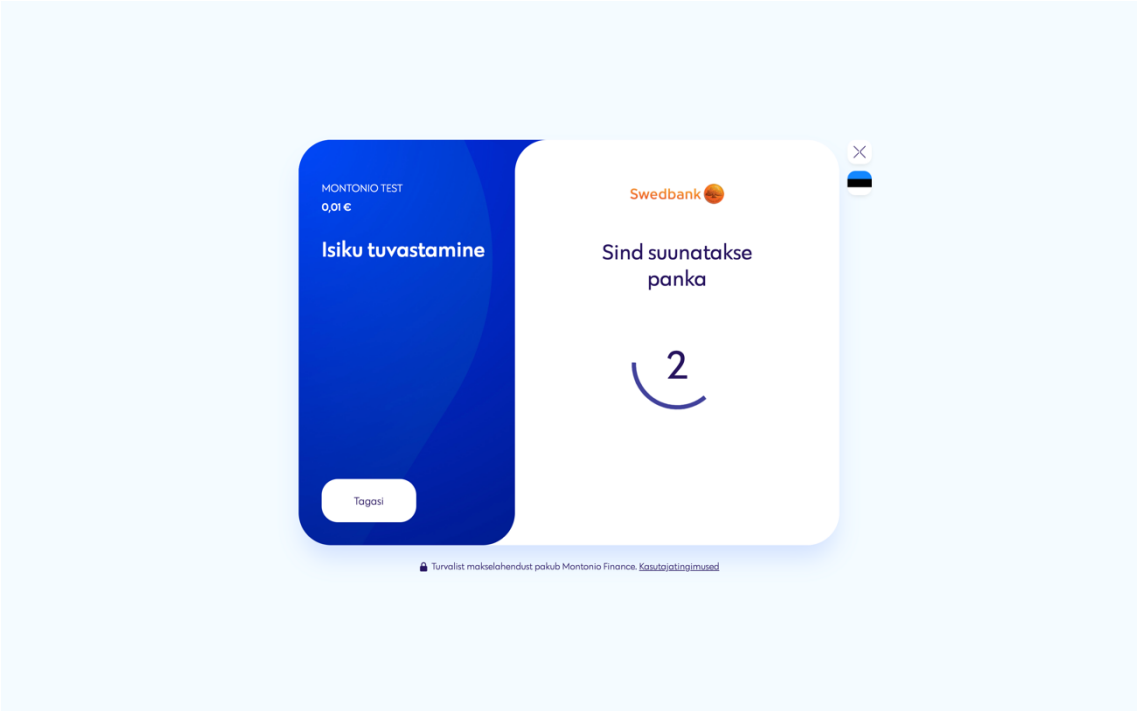
[16] Pangaliit: Avatud pangandus. [WWW] https://pangaliit.ee/arveldused/avatud-pangandus (21.02.2021)

[17] Taltech: Infoturbe poliitika. [WWW] https://oigusaktid.taltech.ee/infoturbe-poliitika/ (21.02.2021)

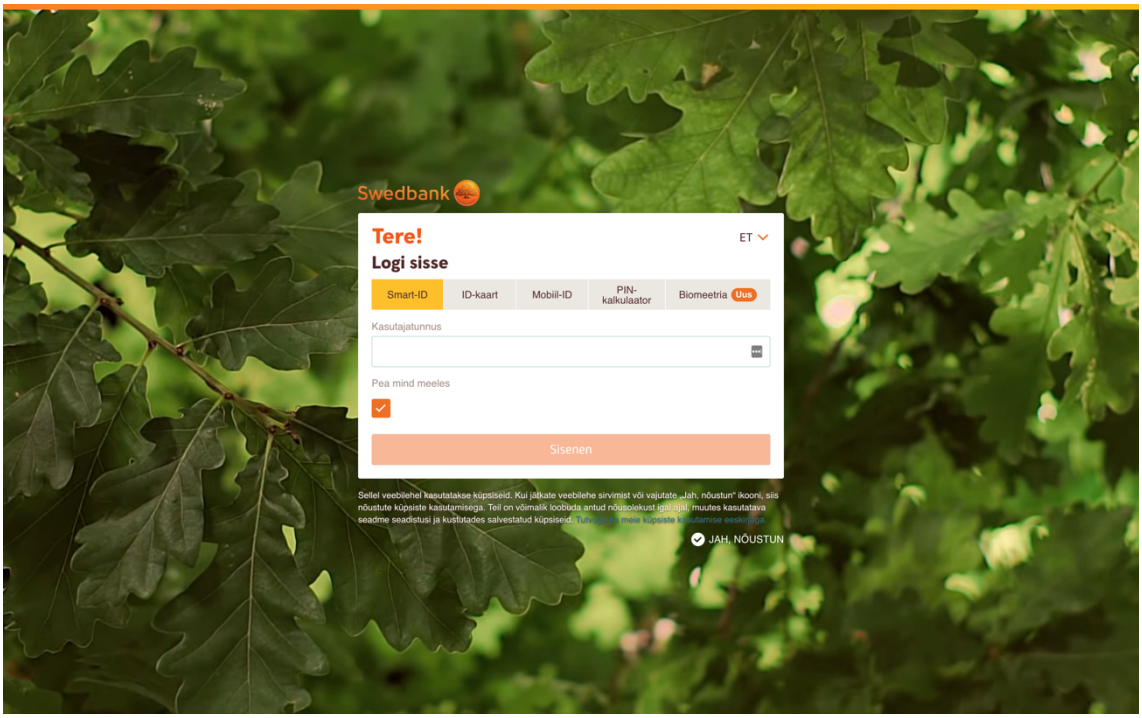
[18] Finantsinspektsioon: Rahapesu tõkestamine. [WWW] https://www.fi.ee/et/finantsinspektsioon/rahapesu-tokestamine (21.02.2021)

[19] Sentry: Working code, happy customers. [WWW] https://sentry.io/about/#:~:text=We're%20so%20much%20more,probably%20a%20few%20therapy%20sessions.
[20] Sentry: Javascript. [WWW] https://docs.sentry.io/platforms/javascript/
[21] LogRocket: Configuration. [WWW] https://docs.logrocket.com/reference#javascript-sdk-api
[22] EveryPay: 3D Secure 2. [WWW] https://every-pay.com/et/3d-secure/

Lisa 1 – Kasutajaliidese vaated

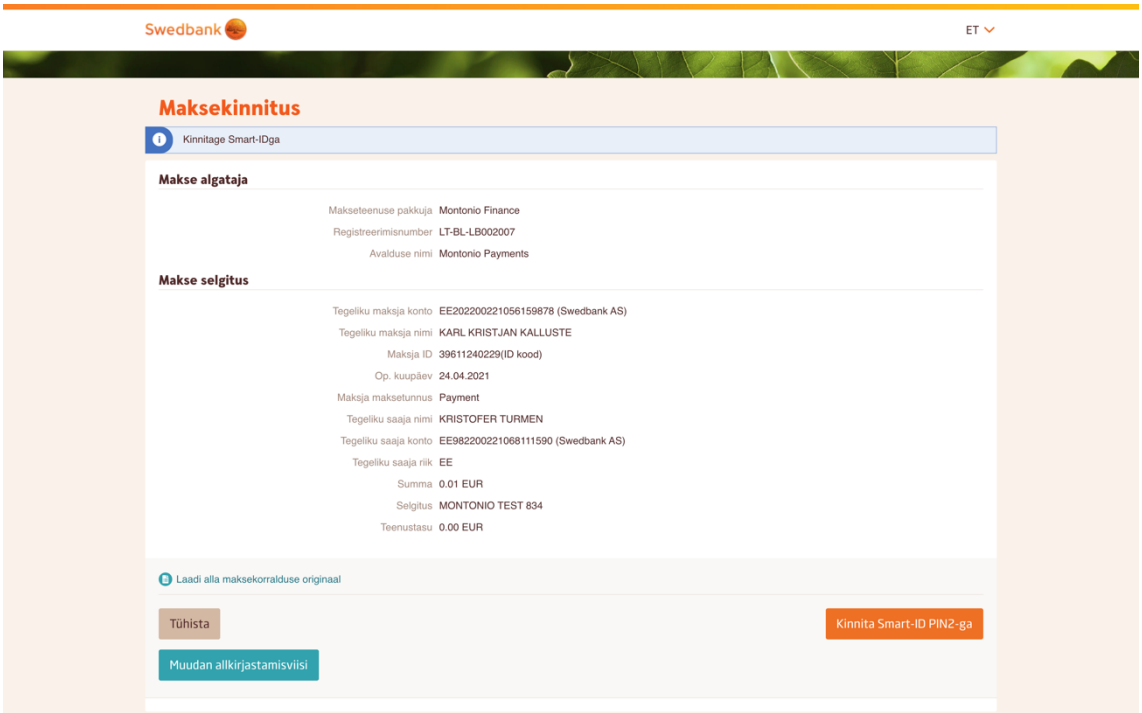


Joonis 15. Kasutajaliides: autentimiseks panga ümbersuunamine



Joonis 16. Autentimine Swedbankis

Joonis 17. Kasutajaliides: makse kinnitamiseks panka ümbersuunamine



Joonis 18. Makse kinnitamine Swedbankis

Lisa 2 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Karl Kristjan Kalluste

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Euroopa makseteenuste direktiivil PSD2 põhineva makse algatamise teenuse loomine" mille juhendaja on Evelin Halling.
   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.

30.04.2021

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 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.