Kauno technologijos universitetas

Informatikos fakultetas

Modulis „Tiriamasis projektas 1“

Projektas: „Savarankiškos suverenios pseudonimizuotos tapatybės valdymo sistema“

Projekto paraiška

IFM 4/2 gr. Danielė Stasiūnaitė
Studentė

Doc. Mindaugas Vasiljevas
Projekto vadovas

Doc. dr. Eglė Butkevičiūtė
Dėstytoja

Kaunas, 2024

Turinys

Įvadas

Skaitmeniniame amžiuje, kai asmens duomenys tampa viena svarbiausių vertybių, privatumo užtikrinimas ir efektyvus tapatybės valdymas yra pagrindiniai iššūkiai, su kuriais turi susidurti ne tik privatūs asmenys, bet ir įvairios organizacijos. Sparčiai augantys informacijos srautai, elektroninių paslaugų plėtra bei kitų paslaugų, reikalaujančių naudotojų autentifikacijos, vystymas lėmė inovatyvių technologinių sprendimų - blokų grandinės pritaikymo, realizuojant decentralizuotos asmens tapatybės valdymo modelį - kūrimą. Pastaruoju sprendimu siekiama užtikrinti asmens duomenų saugumą bei visapusišką duomenų kontrolę, kuri atliekama paties naudotojo.

Šiuo metu egzistuojančios asmens tapatybės valdymo sistemos, pavyzdžiui, centralizuotos ar federacinės, dažnai susiduria su privatumo, duomenų apsaugos ir patogumo iššūkiais. Centralizuotos sistemos yra itin jautrios saugumo pažeidimams, o federacinės sistemos dažnai riboja naudotojo autonomiją. Šie trūkumai skatina naujų sprendimų kūrimo poreikį, orientuotą į naudotojo teisių ir privatumo stiprinimą.

Šis projektas skirtas sukurti savarankiškos suverenios pseudonimizuotos tapatybės valdymo sistemą, kuri leistų naudotojams ne tik valdyti asmeninę informaciją ir dalinimąsi ja, bet ir užtikrintų, kad asmeniniai duomenys negalėtų būti lengvai susieti su naudotoju, kurį šie duomenys apibūdina. Šie tikslai bus pasiekti, pritaikius decentralizuotos tapatybės valdymo modelį, kuris grindžiamas blokų grandinės technologija, duomenų šifravimo bei pseudonimizavimo metodikomis.

Projekto pasiūlymas yra suformuluotas pagal Mindaugo Vasiljevo užsakymą. Projektą numatyta įgyvendinti kaip magistrinio darbo dalį iki 2026 m. birželio mėnesio.

1 Projekto paraiška

1.1 Projekto aprašymas

1.1.1 Projekte analizuojamos problemos

Pagrindinės projekte analizuojamos problemos yra mokslinės literatūros analizės metu identifikuoti savarankiškos suverenios asmens tapatybės valdymo modelio iššūkiai. Šie iššūkiai apima:

- **Blokų grandinės pažeidžiamumus.** Nepaisant to, kad sistemoms, kuriose panaudota blokų grandinės technologija, būdingas decentralizavimas ir skaidrumas, šios sistemos jautrios įvairioms specifinėms atakoms, galinčioms paveikti sistemos saugumą [1].
- **Savarankiškos suverenios tapatybės tinklo plėtrą.** Augant sistemos naudotojų skaičiui sistema turi gebėti apdoroti didelį informacijos kiekį, nepakenkiant sistemos našumui.
- **Suderinamumą su privatumo įstatymais.** Blokų grandinės technologija pasižymi tuo, jog šios grandinės duomenų negalima ištrinti. Dėl šios priežasties sunku įgyvendinti Bendrojo duomenų apsaugos reglamento (BDAR) reikalavimą, nusakantį, kad naudotojas gali pareikalauti, jog jo asmeniniai duomenys būtų ištrinti [2].
- **Programų ir sistemų patogumą**. Egzistuojančiose savarankiškos suverenios tapatybės valdymo sistemose skirta nepakankamai dėmesio naudotojams ir jų naudojimosi sistema patirčiai.

1.1.2 Projekte keliamos hipotezės

Hipotezė: savarankiška suvereni pseudonimizuota asmens tapatybės valdymo sistema pagerins naudotojų kontrolę ir prieigą prie asmeninių duomenų, užtikrindama geresnį duomenų saugumą ir privatumą (lyginant su tradiciniais tapatybės valdymo modeliais).

Aprašymas: blokų grandinės technologijos naudojimas leidžia užtikrinti didesnį duomenų vientisumo ir saugumo lygį, pseudoniminiai identifikatoriai sumažina asmens duomenų atskleidimo riziką. Taip pat savarankiška suvereni asmens tapatybės valdymo sistema suteikia galimybę naudotojui teikti prieigą prie asmeninės informacijos tik tam tikroms grupėms ar asmenims.

1.1.3 Neapibrėžtumai

Projekto neapibrėžtumus gali lemti ne vienas tarpusavyje susijęs veiksnys, apimantis technologinius, naudotojų ir saugumo aspektus. Technologinis neapibrėžtumas gali atsirasti tada, kai pasirinktos technologijos yra nesuderinamos su praktiniais reikalavimais. Tai reiškia, kad priimti sprendimai gali būti efektyvūs tik teoriniame lygmenyje, tačiau bandant šį sprendimą pritaikyti naujos sistemos kūrime galima pastebėti, kad šis sprendimas neatitinka naudotojų poreikių ir nėra tinkamas. Tam, jog būtų mažinama tokio neapibrėžtumo tikimybė, ankstyvosiose sistemos vystymo stadijose bus atliekama detali pasirinktų technologinių sprendimų analizė, įvertintos galimos jų rizikos bei numatyti alternatyvūs sprendimai.

Naudotojų privatumo ir asmens duomenų saugumo užtikrinimas yra vienas iš esminių kuriamos sistemos kriterijų, tačiau dėl netinkamai pasirinktų technologinių sprendimų gali atsirasti privatumo ir duomenų apsaugos spragų (pavyzdžiui, naudotojų informacijos pseudonimizavimui gali būti pasirinkti metodai, kurie gali būti nesunkiai įveikiami, taikant skirtingas įsilaužimo technikas; sistemoje gali būti reikalaujama įvesti perteklinį kiekį asmeninės informacijos). Pastariesiems neapibrėžtumams spręsti nuo pat sistemos kūrimo pradžios turi būti detaliai išanalizuoti pasirinkti metodai bei numatyti alternatyvūs sprendimai. Taip pat turi būti kruopščiai įvertinta, kokie asmeniniai duomenys yra būtini ir be kurių naudojimasis sistema būtų neįmanomas (svarbu atsižvelgti į pagrindinius savarankiškos suverenios asmens tapatybės valdymo principus, aprašytus Kristoferio Aleno [6]). Taip pat turi būti palaikoma reguliari komunikacija su užsakovu, siekiant užtikrinti, kad sistemos funkcijos atitinka naudotojų poreikius.

1.1.4 Projekto apibendrinimas

Toliau pateikiamas vykdomo projekto atitikimas SMART metodologijos principams, kur įrodoma, kad projektas yra: konkretus (angl. *specific*), išmatuojamas (angl. *measurable*), įgyvendinamas (angl. *achievable*), aktualus (angl. *relevant*) ir apibrėžtas laike (angl. *time-bound*).

Konkretus

Konkretus projekto tikslas yra sukurti sistemos, leidžiančios neatskleisti privačios asmens informacijos, prototipą, kuris leistų naudotojams išsaugoti savo privatumą internete.

Išmatuojamas

Objektyvus projekto sėkmingo įgyvendinimo rezultatas įvertinamas konkrečiais kriterijais, kurie gaunami, taikant skirtingas priemones ar metodus:

- 100% numatytų užduočių įgyvendinimas pagal numatytą planą (projekto užduočių specifikavimo ir jų įgyvendinimo etapas). Užduočių atlikimo progresas stebimas, naudojant Microsoft Project.
- 100% tapatybės kūrimo, valdymo, saugojimo ir apsaugos funkcijų komponentų sukūrimas pagal specifikuotus reikalavimus ir 95% klaidų pašalinimas (savarankiškos tapatybės valdymo sistemos kūrimo etapas). Konkrečių užduočių atlikimo kiekis stebimas, palyginus atliktų darbų sąrašą su patvirtintais ir dokumentuotais projekto darbais.
- 95% duomenų sėkmingas šifravimas/dešifravimas (šifravimo sprendimų kūrimo etapas). Tapatybės duomenų šifravimo/dešifravimo korektiškumas patikrinamas, atlikus automatizuotus pseudonimizavimo ir šifravimo testus.
- Testavimo sėkmės rodiklis (99% funkcionalumo tikslumas pagal paruoštą specifikaciją). Funkcionalumo tikslumas įvertinamas, atliekant rankinius ir automatizuotus testus, padedančius įvertinti klaidų ištaisymo efektyvumą.
- Galutinio produkto funkcionalumas ($>$ 70% naudotojų aktyviai naudojasi sistema ir $>$ 80 % naudotojų išreiškė pasitenkinimą sistemos funkcionalumu ir bendra patirtimi). Šis kriterijus įvertinamas, naudojant kokybinius duomenis (įvykdžius naudotojų apklausą apie naudojimosi sistema patirtį ir lūkesčių atitikimą). Taip pat galutinio produkto vertinimas vyksta, atliekant A/B testavimą.

Įgyvendinamas

Projektas yra įgyvendinamas, nes jis yra pagrįstas egzistuojančiais aiškiai apibrėžtais technologiniais blokų grandinės, šifravimo, decentralizuotų protokolų pritaikymo savarankiškos suverenios tapatybės valdymo sistemoje sprendimais. Šios technologijos yra patikrintos įvairiose srityse (pavyzdžiui, finansuose), todėl jų pritaikymas tapatybės valdymui yra realus [4]. Projekto įgyvendinamumą lemia ir tai, jog projektas yra suskirstytas į aiškias planavimo, prototipo kūrimo, testavimo ir sistemos paleidimo fazes, kurios užtikrina nuoseklų ir efektyvų darbą.

Aktualus

Projektas pateikia sprendimą, padedantį spręsti esmines šiuolaikines skaitmeninės visuomenės problemas, susijusias su duomenų apsauga, bei leidžiantį užtikrinti saugų naudotojų tapatybės valdymą.

Apibrėžtas laike

Projektas bus įgyvendintas per 24 mėnesius nuo projekto pradžios. Visas projektas yra suskaidytas į atskiras veiklas, kurios turi būti realizuotos per nustatytus laiko intervalus.

1.2 Pasiūlymas

1.2.1 Technologinės parengties lygiai

Žemiau esančiuose poskyriuose detalizuojami projekto parengties lygiai (nuo 1 iki 7 lygio).

TPL 1: Fundamentinių žinių įgijimas

Numatyta, kad pirmas etapas turi būti įvykdytas per 2 mėnesius. Šiame etape išskiriami šie projekto vystymo uždaviniai:

- **Mokslinės literatūros analizės atlikimas:** ištirti egzistuojančias technologijas ir literatūrą (asmens tapatybės valdymo sistemų apibūdinimas, egzistuojančių modelių apibendrinimas, didžiausią potencialą turinčio - savarankiškos suverenios tapatybės valdymo - modelio aptarimas), kad būtų nustatyti pagrindiniai principai ir technologijos, reikalingos projekto vystymui.
- **Pagrindinių technologijų ištyrimas:** išanalizuoti pagrindinius technologinius sprendimus, tokius kaip pseudonimizacija, šifravimas, decentralizuoti sprendimai (blokų grandinės technologija), kurie gali būti naudojami sistemos kūrime.

Įvykdžius šį etapą bus gauti šie rezultatai:

- Atlikta išsami asmens tapatybės valdymo modelių analizė.
- Išanalizuota blokų grandinės technologija, kuri bus taikoma, kuriant savarankiškos suverenios tapatybės valdymo sistemos prototipą.

TPL 2: Žinių taikymo koncepcijos formulavimas

Numatyta, kad antras etapas turi būti įvykdytas per 3 mėnesius. Šiame etape išskiriami šie projekto vystymo uždaviniai:

- **Technologinių sprendimų pasirinkimas:** iš išanalizuotų technologijų pasirinkti tinkamiausius sprendimus, kurie bus naudojami sistemos kūrime.
- **Problemos analizė:** identifikuoti iššūkius ir problemas, su kuriomis gali tekti susidurti diegiant pasirinktą technologiją.

Įvykdžius šį etapą bus gauti šie rezultatai:

- Nustatyta, kuri technologija geriausiai atitinka projekto tikslus ir kokie yra jos privalumai bei trūkumai.
- Identifikuoti pagrindiniai sistemos vystymo iššūkiai ir jų sprendimo būdai.

TPL 3: Koncepcijos įgyvendinamumo įrodymas / patvirtinimas

Numatyta, kad trečias etapas turi būti įvykdytas per 5 mėnesius. Šiame etape išskiriami šie projekto vystymo uždaviniai:

- **Prototipo kūrimas ir testavimas:** sukurti pirmąjį savarankiškos suverenios tapatybės valdymo sistemos prototipą ir atlikti testus.
- **Technologijų įgyvendinamumo vertinimas:** patikrinti, ar pasirinktų technologijų (blokų grandinės, kriptografijos, pseudonimizacijos) derinys leidžia pasiekti pagrindinius sistemos tikslus - saugumą ir asmens duomenų privatumą.
- **Sistemos funkcionalumo vertinimas:** patikrinti, ar sistemos prototipas užtikrina naudotojo tapatybės valdymo galimybes be pašalinių suinteresuotų šalių įsikišimo (ar veikia decentralizuotu principu). Taip pat siekama įvertinti, ar prototipas atitinka naudotojo poreikius.

Įvykdžius šį etapą bus gauti šie rezultatai:

- Nustatyta, kad prototipas atitinka projekto koncepciją ir leidžia pasiekti numatytus tikslus.
- Įrodyta, kad pasirinktos technologijos gali būti pritaikytos realizuojant asmens tapatybės valdymo sistemą.
- Parengtos testavimo ataskaitos, kuriose aprašyti ištestuoti testavimo scenarijai, pasiekti rezultatai, identifikuotos problemos bei galimi jų sprendimo būdai.
- Pateiktos išvados dėl sistemos optimizavimo ir tobulinimo poreikio.

TPL 4: Maketo (modelio), meno objekto projekto kūrimas ir testavimas

Numatyta, kad ketvirtas etapas turi būti įvykdytas per 5 mėnesius. Šiame etape išskiriami šie projekto vystymo uždaviniai:

- **Maketo (modelio) sukūrimas:** sukurti pirmąjį sistemos maketą, kuris apims pagrindines savarankiškos suverenios tapatybės valdymo funkcijas (tapatybės kūrimas, autentifikacija, saugumo mechanizmai, pseudonimizacija).
- **Naudotojo sąsajos kūrimas (UI/UX):** kuriant maketą atsižvelgti į tai, kad sistema turi būti suprantama, patogi ir intuityvi naudoti, todėl turi būti skiriamas didesnis dėmesys naudotojo patirčiai (UI/UX dizainui).
- **Funkcionalumo testavimas:** atlikti įvairius testus, siekiant patikrinti, ar sistemoje realizuotas patvirtintas funkcionalumas.

- **A/B testavimas:** atlikti A/B testavimą, siekiant įvertinti, kuri naudotojo sąsajos versija yra efektyvesnė ir priimtinesnė naudotojui.

Įvykdžius šį etapą bus gauti šie rezultatai:

- Sukurtas sistemos maketas, vaizduojantis sistemos pagrindines funkcijas ir naudotojo sąsają.
- Parengta ataskaita apie atliktus testus ir gautus rezultatus, įvertinant, ar maketas atitinka naudotojo poreikius ir patvirtintus sistemos reikalavimus.

TPL 5: Maketo (modelio) patikrinimas imituojant realias sąlygas, meno objekto projekto pristatymas visuomenei

Numatyta, kad penktas etapas turi būti įvykdytas per 2 mėnesius. Šiame etape išskiriami šie projekto vystymo uždaviniai:

- **Modelio pristatymas:** pristatyti sukurtą sistemos maketą (su realizuotu nepilnu sistemos funkcionalumu) kitiems suinteresuotiems asmenims.
- **Grįžtamojo ryšio surinkimas ir įvertinimas:** surinkti naudotojų nuomones apie sistemą ir, esant poreikiui, atlikti reikalingus sistemos tobulinimo darbus.
- **Testavimo duomenų rinkimas:** rinkti duomenis apie sistemos veikimą realiomis sąlygomis (realios sąlygos yra simuliuojamos), įskaitant naudotojų atsiliepimus ir sistemos elgsenos stebėjimą, siekiant įvertinti jos trūkumus.

Įvykdžius šį etapą bus gauti šie rezultatai:

- Gauti naudotojų grįžtamojo ryšio rezultatai.
- Sudarytas sistemos naudotojų identifikuotų sistemos trūkumų sąrašas.
- Atlikti sistemos tobulinimo darbai, atsižvelgus į naudotojų grįžtamąjį ryšį.

TPL 6: Prototipo (bandomosios versijos) kūrimas

Numatyta, kad šeštas etapas turi būti įvykdytas per 5 mėnesius. Šiame etape išskiriami šie projekto vystymo uždaviniai:

- **Prototipo kūrimas:** sukurti pirmąją pilnai funkcionuojančią sistemos versiją, kurioje bus realizuotos visos pagrindinės funkcijos - asmens tapatybės sukūrimas, autentifikacija, pseudonimizacija ir saugumo mechanizmai.

- **Testavimas su realiais duomenimis:** išbandyti prototipą su tikrais duomenimis ir realiais naudojimosi sistema scenarijais, kad būtų įvertinta, kaip sistema veikia realioje aplinkoje.
- **Grįžtamojo ryšio surinkimas ir įvertinimas:** surinkti naudotojų nuomones apie sistemą ir, esant poreikiui, atlikti reikalingus sistemos tobulinimo darbus.
- **Našumo testavimas:** patikrinti, kaip veikia sistemos prototipas, kai juo naudojasi didelis naudotojų srautas (ne mažiau nei 100 naudotojų).

Įvykdžius šį etapą bus gauti šie rezultatai:

- Sukurtas pilnai funkcionuojantis sistemos prototipas, apimantis visas pagrindines funkcijas, kurios yra būtinos savarankiškos suverenios tapatybės valdymo sistemos veikimui.
- Atlikti testavimai ir surinktas naudotojų grįžtamasis ryšys, kurį įvertinus atlikti reikalingi sistemos tobulinimo darbai.
- Parengta sistemos prototipo našumo ataskaita, kurioje aprašytas sistemos gebėjimas veikti efektyviai ir be trikdžų, kai sistema naudojasi didelis naudotojų srautas.

TPL 7: Prototipo (bandomosios versijos) demonstravimas

Numatyta, kad septintas etapas turi būti įvykdytas per 2 mėnesius. Šiame etape išskiriami šie projekto vystymo uždaviniai:

- **Prototipo demonstravimas suinteresuotoms šalims:** pademonstruoti sistemos prototipą suinteresuotoms šalims.
- **Testavimas realiomis sąlygomis:** atlikti demonstravimus su realiais sistemos naudotojais ir surinkti jų atsiliepimus apie sistemos funkcionalumą ir patogumą (skiriant daugiau dėmesio ir naudotojo sąsajos testavimui). Esant poreikiui atlikti sistemos pakeitimus ir identifikuoti kitas sistemos tobulinimo galimybes.
- **Ataskaitos parengimas:** parengti ataskaitą apie atliktą prototipo demonstravimą (įskaitant gautus galutinių naudotojų atsiliepimus ir reikalingus sistemos pakeitimus).

Įvykdžius šį etapą bus gauti šie rezultatai:

- Pademonstruotas sistemos veikimas realiomis sąlygomis.
- Surinktas ir išanalizuotas galutinių naudotojų grįžtamasis ryšys (esant poreikiui atlikti reikalingi sistemos prototipo pakeitimai).
- Parengta savarankiškos suverenios asmens tapatybės valdymo sistemos prototipo kokybės vertinimo ataskaita.

1.2.2 Rizika ir apribojimai

Skirtinguose savarankiškos suverenios pseudonimizuotos tapatybės valdymo sistemos projekto etapuose (TPL lygiuose) gali kilti specifinės rizikos, kurių mažinimui arba eliminavimui būtina numatyti atitinkamus veiksmus. Pagrindinės projekto rizikos ir jų mažinimo veiksmai aprašyti žemiau pateiktuose poskyriuose pagal TPL lygius.

Koncepcijos įgyvendinamumo įrodymo/patvirtinimo etapo (TPL3) rizikos

1. **Rizika:** nepakankamai detaliai paruošta sistemos funkcionalumo specifikacija.

Kritiniai taškai:	**Rizikų mažinimo veiksmai:**
• **Pradinės specifikacijos versijos parengimas.** Specifikacija turi būti kuo išsamesnė, jog būtų išvengta nesusipratimų ir klaidų projekto vystymo eigoje. • **Poreikių analizė su užsakovu.** Turi būti atlikta visapusiška užsakovo poreikių analizė, jog vėlesniuose sistemos vystymo etapuose nekiltų nesusipratimų dėl neteisingai suprastų ir realizuotų užsakovo poreikių.	• Periodinės specifikacijos peržiūros ir patikros su užsakovu. • Kurti ankstyvus sistemos prototipus, kad būtų galima praktiškai patikrinti reikalavimus.

2. **Rizika:** neatitikimai tarp teorinių galimybių ir praktinio įgyvendinimo.

Kritiniai taškai:	**Rizikų mažinimo veiksmai:**
• **Technologinių sprendimų priėmimas.** Pasirinkti technologiniai sprendimai gali būti itin sudėtingi ir sunkiai įgyvendinami. Pasirinkti teoriniai technologiniai sprendimai remiasi paprastesniais arba idealiais scenarijais, kurie nebūtinai atspindi realias sistemos sąlygas. • **Resursų paskirstymas.** Sistemos vystymo eigoje gali paaiškėti, kad technologiniams sprendimams realizuoti reikia daugiau resursų (laiko ir žinių).	• Patikrinti teorinių modelių atitikimą praktinėms sąlygoms (naudojant maketus). • Testuoti prototipus naudotojų aplinkoje, siekiant identifikuoti neatitikimus tarp teorijos ir praktikos. • Rinkti statistinius duomenis apie sistemos našumą, saugumą ir kitus kritinius rodiklius. • Organizuoti projektavimo komandos ir užsakovo bendras peržiūras.

Maketo (modelio), meno objekto projekto kūrimo ir testavimo etapo (TPL4) rizikos

1. **Rizika:** nepakankamas sistemos funkcionalumų įvertinimas.

Kritiniai taškai:	**Rizikų mažinimo veiksmai:**
• **Prioritetinių funkcijų analizė.** Pradiniame sistemos realizavimo etape gali būti neteisingai apibrėžtos prioritetinės sistemos funkcijos, todėl ankstyvojoje sistemos vystymo stadijoje gali būti realizuotos neesminės funkcijos. • **Neprioritetinių funkcijų analizė.** Sistemos funkcionalumai gali būti netinkamai aprašyti, todėl gali būti netinkamai suplanuotas projekto veiklų vykdymas ir netinkamai numatytas laikas joms atlikti.	• Sudaryti prioritetinių funkcionalumų sąrašą, konsultuojantis su užsakovu. • Ankstyvosiose sistemos vystymo stadijose išsamiai aprašyti visas sistemos funkcijas bei aptarti jas su užsakovu (gauti patvirtinimą).

Maketo patikrinimo imituojant realias sąlygas etapo (TPL5) rizikos

1. **Rizika:** modelio veikimo neatitikimas realioms sąlygoms.

Kritiniai taškai:	**Rizikų mažinimo veiksmai:**
• **Testavimo plano parengimas.** Šis planas gali neapimti svarbių scenarijų, su kuriais sistema gali susidurti realioje aplinkoje. • **Tikėtinų modelio rezultatų pateikimas.** Sistemos modelis gali netinkamai prognozuoti realų naudotojų elgesį - naudotojai gali elgtis kitaip nei buvo numatyta sistemos vystymo eigoje, todėl sistema gali neatitikti naudotojų lūkesčių.	• Sukurti išsamų ir realias sąlygas atspindintį testavimo planą. • Patikrinti kelis modelio veikimo scenarijus.

2. **Rizika:** nepakankamas testavimo lygis, kas gali lemti klaidų neaptikimą (klaidos išryškėja tik vėlesniuose vystymo etapuose).

Kritiniai taškai:	**Rizikų mažinimo veiksmai:**
• **Testavimo planavimas.** Testavimas turi būti atliekamas jau ansktyvosiose sistemos vystymo stadijose, jog klaidos būtų aptinkamos kuo anksčiau (tuo atveju, jei testavimas atliekamas per vėlai, dalis klaidų gali būti nepastebėta dėl sistemos sudėtingumo ir kompleksiškumo). • **Testavimo scenarijų kūrimas.** Klaidos gali būti nepastebėtos, jei pateikiamas nepakankamai detalus testavmo scenarijų įvairovės ir detalumo aprašymas (dalis sistemos panaudojimo atvejų gali likti neištestuoti).	• Naudoti testavimo metodikas, užtikrinančias plačią aprėptį (vienetinius testus). • Detaliai aprašyti testavimo scenarijus, kurie padengtų sukurtą sistemos funkcionalumą. • Patvirtinti testavimo scenarijus su užsakovu.

Prototipo kūrimo etapo (TPL6) rizikos

1. **Rizika:** resursų (laiko, biudžeto, komandos kompetencijų) trūkumas, kas gali lemti vėlavimus.

Kritiniai taškai:	**Rizikų mažinimo veiksmai:**
• **Resursų paskirstymas.** Projektas gali būti pradedamas be tinkamai paskirstytų resursų, todėl tai gali lemti projekto veiklų ir galutinio produkto pateikimo vėlavimus.	• Detaliai suplanuoti užduotis ir jų atlikimo terminus. • Prioritetą skirti svarbiausių sistemos funkcijų realizavimui. • Reguliariai susitikti su užsakovu ir pristatyti projekto progresą.

2. **Rizika:** Sistemos prototipas gali būti testuojamas sąlygomis, kurios neatspindi tikrų naudojimo scenarijų.

Kritiniai taškai:	**Rizikų mažinimo veiksmai:**
• **Testavimo scenarijų kūrimas.** Gali būti sukurti tokie testavimo scenarijai, kurie naudoja netinkamus duomenis, nepaiso techninių apribojimų arba nesimuliuoja realios sistemos naudojimo sąlygų. Tai gali lemti netikslius ir neišsamius sistemos funkcionalumo testavimo rezultatus.	• Simuliuoti realias darbo sąlygas, naudojant emuliatorius ar virtualias aplinkas. • Testavimą vykdyti su realiais naudotojais. • Dokumentuoti visus testų rezultatus ir juos analizuoti.

Prototipo demonstravimo etapo (TPL7) rizikos

1. **Rizika:** nepilnai suprasti užsakovo poreikiai.

Kritiniai taškai:	**Rizikų mažinimo veiksmai:**
• **Užsakovo poreikų supratimas.** Nepakankama komunikacija su užsakovu gali sukelti klaidingą projekto supratimą ir klaidingus lūkesčius apie sistemos galimybes ir funkcionalumą. • **Testavimo atlikimas ir grįžtamojo ryšio teikimas.** Užsakovo poreikiai gali būti nepilnai išsiaiškinti. Taip pat gali būti nepateiktas grįžtamasis ryšys apie konkrečias realizuotas sistemos funkcijas. Dėl šių priežasčių sistemos prototipas gali būti testuojamas pagal netinkamus kriterijus, kurie netenkina realių užsakovo poreikių.	• Įtraukti tikslinius naudotojus į ankstyvus sistemos testavimus. • Sukurti demonstracijos scenarijus, atspindinčius realius sistemos naudojimo atvejus. • Ansktyvosiose sistemos vystymo stadijose rinkti grįžtamąjį ryšį ir, esant poreikiui, atlikti sistemos pakeitimus prieš prototipo demonstraciją.

1.2.3 Projekto biudžetas

Žemiau esančioje lentelėje (1 lentelė) pateikiamas projekto biudžeto skaičiavimas.

1 lentelė. Projekto biudžeto skaičiavimas.

Išlaidos	Vienetas	Vienetų skaičius	Vieneto kaina, Eur	Viso, Eur
1. Žmonių ištekliai				
Projekto vadovas	Mėnesis	24	3 100	74 400
Programuotojas	Mėnesis	24	1 700	40 800
Iš viso žmonių išteklių				115 200
2. Įranga ir prekės				
Kompiuterio pelytė	Vienetas	1	25	25
Kompiuteris	Vienetas	1	980	980
Monitorius	Vienetas	1	120	120
Iš viso įranga ir prekės				1 125
3. Programinė įranga				
Linux operacinė sistema	Vienetas	1	0	0
Visual Studio Code	Vienetas	1	0	0
MagicDraw	Vienetas	1	181	181
Microsoft Project	Licencija (metams)	2	112,80	225,6
Iš viso programinė įranga				406,6
4. Viso tiesioginiai projekto kaštai				**116 731,6**

1.2.4 Produkto rinkos aprašymas

Skaitmeninės tapatybės valdymo rinka sparčiai auga ir yra viena iš pagrindinių technologijų sričių, kurios plėtrą skatina didėjantis privatumo ir duomenų apsaugos poreikis [3]. Pagal pasaulinės rinkos tyrimus prognozuojama, kad 2025 m. rinkos vertė pasieks 119.80 mlrd. JAV dolerių ir iki 2032 m. rinkos vertė ims viršyti 807 mlrd. JAV dolerius. Remiantis šaltiniu pagrindiniai rinkos augimą lemiantys veiksniai yra didėjanti kibernetinių atakų grėsmė, elektroninės prekybos plėtra, augančios nuotolinio darbo galimybės, daiktų interneto ir blokų grandinių technologijų vystymasis [7]. Prie augančios rinkos prisideda ir griežtėjančių teisinių aktų, pavyzdžiui, Bendrojo duomenų apsaugos reglamento (BDAR) keliami reikalavimai Europos Sąjungoje įsteigtoms organizacijoms, tvarkančioms asmens duomenis [8].

Šiuo metu rinkoje egzistuoja centralizuotos, federacinės ir decentralizuotos (savarankiškos suverenios tapatybės) asmens tapatybės valdymo sistemos. Centralizuotos sistemos leidžia naudotojams autentifikuotis, naudojant vieną platformą, tačiau kelia rimtų privatumo rizikų dėl galimo neteisėto duomenų panaudojimo ir jų nutekinimo (kaip kad 2021 m. nutiko 533 mln. centralizuotą tapatybės valdymo sistemą naudojančio „Facebook“ naudotojų, kurių asmeniniai duomenys buvo nutekinti [9]). Federacinės sistemos, tokios kaip „SAML“ arba „OpenID Connect“, suteikia daugiau lankstumo tarp organizacijų, bet vis tiek remiasi centralizuotais valdymo elementais. Decentralizuotos sistemos, kurios tampa vis populiaresnės, pavyzdžiui, „Sovrin“ arba „uPort“, siūlo savarankiškos tapatybės valdymo sprendimus, paremtus blokų grandinės technologijomis [1] ir leidžiančius naudotojams visiškai kontroliuoti savo tapatybės duomenis.

Egzistuojančioms sistemoms būdingos kelios problemos, apimančios duomenų privatumo ir saugumo užtikrinimą bei sudėtingai realizuojamą naudotojams priimtinų ir jų poreikius atitinkančių sprendimų įgyvendinimą. Šiame projekte kuriama savarankiškos suverenios pseudonimizuotos tapatybės valdymo sistema siekiama išspręsti šias egzistuojančių sistemų problemas, siūlydama į naudotoją orientuotus decentralizuotos sistemos modelio sprendimus, leidžiančius naudotojams valdyti savo tapatybės duomenis pseudonimizuotu būdu, ir asmeninių duomenų saugumo užtikrinimą.

1.2.5 Santrauka

Vertėmis grįstas pasiūlymas: sistema leis naudotojams valdyti asmeninius duomenis ir išsaugoti privatumą internete. Kitaip nei egzistuojančios sistemos, kuriama sistema ne tik naudos decentralizuoto asmens tapatybės valdymo modelio principus, bet ir užtikrins papildomą duomenų saugumą, taikant asmeninės informacijos pseudonimizavimą.

Siūlomas pasiūlymas: bus sukurta sistema, pagrįsta asmeninių duomenų pseudonimizavimu bei blokų grandinės technologija, užtikrinančia decentralizuotą duomenų valdymą.

Literatūros sąrašas

[1] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 113436-113481, 2022, doi: 10.1109/ACCESS.2022.3216643.

[2] Kondova, Galia and Erbguth, Jörn, Self-Sovereign Identity on Public Blockchains and the GDPR (April 1, 2020). Proceedings of ACM SAC Conference, Brno, Czech Republic, March 30- April 3, 2020 (SAC'20), 342 - 345. DOI: 10.1145/3341105.3374066. Prieiga per internetą: https://ssrn.com/abstract=3515213 [žiūrėta 2025-01-12].

[3] Stockburger, L.; Kokosioulis, G.; Mukkamala, A.; Mukkamala, R.; Avital, M. Blockchain-enabled Decentralized Identity Management: The Case of Self-sovereign Identity in Public Transportation. Blockchain Res. Appl. 2021, 2, 100014.

[4] P. Treleaven, R. Gendal Brown and D. Yang, "Blockchain Technology in Finance," in Computer, vol. 50, no. 9, pp. 14-17, 2017, doi: 10.1109/MC.2017.3571047.

[5] Lietuvos Respublikos Seimas, Lietuvos Respublikos viešųjų pirkimų įstatymo Nr. I-1491 pakeitimo įstatymas. Nr. X-1469, 2008-07-03 [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.426659 [žiūrėta 2025-01-12].

[6] Dib, Omar and Toumi, Khalifa, Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions (December 20, 2020). Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 19-40, Vol. 4, No. 5 (2020), Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2020.05.002. Prieiga per internetą: https://ssrn.com/abstract=3785452 [žiūrėta 2025-01-12].

[7] Market Research Future, "Digital Identity Market Research Report - Forecast 2032", Market Research Future [interatyvus]. Prieiga per internetą: https://www.marketresearchfuture.com/reports/digital-identity-market-12149 [žiūrėta 2025-01-12].

[8] Europos Parlamentas ir Taryba, Bendrasis duomenų apsaugos reglamentas (BDAR), Reglamentas (ES) 2016-679 [interaktyvus]. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016R0679 [žiūrėta 2025-01-12].

[9] Goel, A.; Rahulamathavan, Y. A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility. Future Internet 2025, 17, 1. Prieiga per internetą: https://doi.org/10.3390/fi17010001 [žiūrėta 2025-01-12].