



**Kauno technologijos universitetas**

Informatikos fakultetas

## **Modulis „Tiriamasis projektas 2“**

**Projektas: „Savarankiškos suverenios pseudonimizuotos  
tapatybės valdymo sistema“**

Reikalavimų specifikavimas

**IFM 4/2 gr. Danielė Stasiūnaitė**  
Studentė

**Doc. Mindaugas Vasiljevas**  
Projekto vadovas

**Doc. dr. Eglė Butkevičiūtė**  
Dėstytoja

**Kaunas, 2025**

# Turinys

<b>1</b>	<b>Sistemos paskirtis</b>	<b>3</b>
1.1	Projekto kūrimo pagrindas (pagrindimas) . . . . .	3
1.2	Sistemos tikslai (paskirtis) . . . . .	3
<b>2</b>	<b>Užsakovai, pirkėjai ir kiti sistema suinteresuoti asmenys</b>	<b>4</b>
2.1	Užsakovas . . . . .	4
2.2	Pirkėjas . . . . .	4
2.3	Naudotojai . . . . .	4
<b>3</b>	<b>Apribojimai</b>	<b>6</b>
3.1	Apribojimai sprendimui . . . . .	6
3.2	Diegimo aplinka . . . . .	6
3.3	Komunikuojančios sistemos . . . . .	6
3.4	Komerciniai specializuoti programų paketai . . . . .	6
3.5	Numatoma darbo vietos aplinka . . . . .	7
3.6	Sistemos kūrimo terminai . . . . .	8
3.7	Sistemos kūrimo biudžetas . . . . .	8
<b>4</b>	<b>Terminų žodynas</b>	<b>9</b>
<b>5</b>	<b>Svarbūs faktai ir prielaidos</b>	<b>10</b>
<b>6</b>	<b>Veiklos sfera</b>	<b>10</b>
6.1	Veiklos kontekstas . . . . .	10
6.2	Veiklos padalinimas . . . . .	10
<b>7</b>	<b>Produkto veiklos sfera</b>	<b>11</b>
7.1	Sistemos ribos . . . . .	11
7.2	Panaudojimo atvejų sąrašas . . . . .	11
<b>8</b>	<b>Funkciniai reikalavimai ir reikalavimai duomenims</b>	<b>13</b>
8.1	Funkciniai reikalavimai . . . . .	13
8.2	Reikalavimai duomenims . . . . .	20
8.2.1	Duomenų modelis . . . . .	20
8.2.2	Duomenų modelio specifikacija . . . . .	20
<b>9</b>	<b>Reikalavimai sistemos išvaizdai</b>	<b>21</b>
<b>10</b>	<b>Reikalavimai panaudojamumui</b>	<b>22</b>

<b>11 Reikalavimai vykdymo charakteristikoms</b>	<b>23</b>
<b>12 Reikalavimai saugumui</b>	<b>24</b>
<b>13 Teisiniai reikalavimai</b>	<b>25</b>
<b>14 Naujos problemos</b>	<b>26</b>
14.1 Problemos diegimo palinkai . . . . .	26
14.2 Įtaka jau instaliuotoms sistemoms . . . . .	26
14.3 Neigiamas vartotojų nusiteikimas . . . . .	26
14.4 Kliudantys diegimo aplinkos apribojimai . . . . .	26
14.5 Galimos naujos sistemos sukeltos problemos . . . . .	26
<b>15 Uždaviniai</b>	<b>27</b>
15.1 Sistemos pateikimo žingsniai (etapai) . . . . .	27
15.2 Vystymo etapai . . . . .	27
<b>16 Rizikos ir jų valdymas</b>	<b>28</b>
<b>17 Kaina</b>	<b>29</b>
<b>18 Naudotojo dokumentacija</b>	<b>29</b>

# 1 Sistemos paskirtis

## 1.1 Projekto kūrimo pagrindas (pagrindimas)

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.

## 1.2 Sistemos tikslai (paskirtis)

Sistemos kūrimo projektu siekiama įgyvendinti šiuos tikslus:

- 1
- 2
- 3
- 4
- 5

## 2 Užsakovai, pirkėjai ir kiti sistema suinteresuoti asmenys

### 2.1 Užsakovas

Sistemos kūrimo projektą užsako darbo vadovas Mindaugas Vasiljevas. Užsakovo rolės projekte apima sistemos finansavimo, reikalavimų sistemai rinkimo ir teikimo bei konsultacijų, susijusių su dalykine sritimi, teikimą. Darbo vadovo kontaktiniai duomenys:

1 lentelė. Panaudojimo atvejo specifikacija Nr.2.

<b>Mobilusis telefonas:</b>	+37066428763.
<b>El. pašto adresas</b>	mindaugas.vasiljevas@ktu.lt.
<b>Adresas</b>	XI rūmai 3C2b korpusas.
<b>Informacijos galima teirautis</b>	I - V; 10:00 - 17:00.

### 2.2 Pirkėjas

Sistemos pirkėjas sutampa su sistemos užsakovu.

### 2.3 Naudotojai

Žemiau yra pateikiami potencialių sistemos naudotojų - pacientų, gydytojų ir tyrėjų - aprašymai kartu su šių naudotojų charakteristikomis.

#### Pacientai

<b>Funkcijos</b>	Valdyti savo asmeninių genetinių duomenų prieinamumą kitoms naudotojų grupėms; esant poreikiui, įkelti genetinius duomenis; peržiūrėti analizių, atliktų su genetiniais duomenimis, rezultatus.
<b>Patirtis dalykinėje srityje</b>	Žema.
<b>Patirtis IT srityje</b>	Žema.
<b>Papildomos charakteristikos</b>	Sistema besinaudojančius pacientus sieja kalba (lietuvių kalba) ir interesai (valdyti savo asmeninius genetinius duomenis, kurie gali būti panaudoti, net tik atliekant asmens genetinius tyrimus, bet ir moksliniais tikslais).
<b>Prioritetas</b>	Aukštas.

## Gydytojai - genetikai

<b>Funkcijos</b>	Įkelti pacientų genetinius duomenis; atlikti genetinių duomenų analizės ir jų rezultatus pateikti pacientams; gavus leidimą iš paciento perduoti genetinius duomenis tyrėjams.
<b>Patirtis dalykinėje srityje</b>	Aukšta.
<b>Patirtis IT srityje</b>	Vidutinė.
<b>Papildomos charakteristikos</b>	Gydytojus - genetikus sieja išsilavinimas (aukštasis - universitetinis), darbo pobūdis (pacientų genetinių duomenų apdorojimas) ir dalykinė sritis (sveikatos priežiūra).
<b>Prioritetas</b>	Aukštas.

## Tyrėjai

<b>Funkcijos</b>	Atlikti išsamesnes genetinių duomenų analizės (genetinius duomenis apdorojant su specializuotais įrankiais) ir jų rezultatus pateikti gydytojams - genetikams.
<b>Patirtis dalykinėje srityje</b>	Aukšta.
<b>Patirtis IT srityje</b>	Aukšta.
<b>Papildomos charakteristikos</b>	Tyrėjus sieja išsilavinimas (aukštasis - universitetinis), darbo pobūdis (pacientų genetinių duomenų apdorojimas) ir dalykinė sritis (moksliniai tyrimai).
<b>Prioritetas</b>	Aukštas.

## **3 Apribojimai**

### **3.1 Apribojimai sprendimui**

Kuriama sistema turi būti kuriama Windows 10 ar vėlesnių operacinės sistemos versijų pagrindu.

### **3.2 Diegimo aplinka**

### **3.3 Komunikuojančios sistemos**

Sistemos komunikacija su gretimomis sistemomis nėra numatyta.

### **3.4 Komerciniai specializuoti programų paketai**

Užsakovo nurodymu kuriama sistema turi veikti reliacinės duomenų bazės valdymo sistemos Microsoft Server pagrindu.

### 3.5 Numatoma darbo vietos aplinka

Numatomiems sistemoms naudotajams - pacientams, gydytojams ir tyrėjams - būdingos žemiau aprašytos darbo vietos charakteristikos.

**2 lentelė. Numatomos naudotojų darbo vietos aplinkos aprašymai.**

<b>Naudotojas</b>	<b>Aprašymas</b>
Pacientai	Vietoje, kurioje yra sistemos svečias, gali būti silpnas arba spartus internetas.
Gydytojai - genetikai	<ul style="list-style-type: none"><li>• Asmenys naudojami sistema gerai apšviestuose vieno asmens kabinetuose, leidžiančių užtikrinti pacientų konfidencialumą konsultacijų metu.</li><li>• Kabinetuose kompiuteriai išdėstyti taip, kad pacientai negali matyti gydytojo kompiuterio ekrano.</li><li>• Kabinetuose užtikrintas spartus internetas.</li></ul>
Tyrėjai	<ul style="list-style-type: none"><li>• Asmenys naudojami sistema gerai apšviestuose kelių asmenų kabinetuose.</li><li>• Kabinetuose tyrėjų darbataliai su kompiuteriais yra išdėstyti taip, kad darbuotojai nemato vienas kito kompiuterių.</li><li>• Aplinkoje užtikrintas spartus internetas.</li><li>• Kabinetai turi ribotą fizinę prieigą - yra kortelinė durų kontrolės sistema.</li></ul>



### **3.6 Sistemos kūrimo terminai**

Sistema turi būti realizuota iki 2026 m. birželio X dienos.

### **3.7 Sistemos kūrimo biudžetas**

Sistemos kūrimui skiriamas 120 000 eurų biudžetas, tačiau, esant poreikiui, biudžetas gali būti didinamas iki 150 000 eurų.

## 4 Terminų žodynas

Specifikacijoje naudojamos šios santrumpos bei sąvokos:

- **BDAR reikalavimai** - nuo 2018 m. gegužės 25 d. pradėtas taikyti 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

## 5 Svarbūs faktai ir prielaidos

Svarbūs faktai ir prielaidos nebuvo identifikuoti.

## 6 Veiklos sfera

### 6.1 Veiklos kontekstas

X paveiksle () pateikiama veiklos konteksto diagrama.

### 6.2 Veiklos padalinimas

Veiklos konteksto diagramos () srautų apibūdinimas:

## 7 Produkto veiklos sfera

### 7.1 Sistemos ribos

Žemiau esančiame paveiksle pavaizduota sistemos panaudojimo atvejų diagrama:



1 pav.: Panaudojimo atvejų modelis (PAM).

### 7.2 Panaudojimo atvejų sąrašas

Žemiau yra pateiktas panaudojimo atvejų sąrašas, kuris turi būti realizuotas savarankiškos suverenios pseudonimizuotos tapatybės valdymo sistemoje.

- PA1:** Užsiregistruoti sistemoje skirtingų kategorijų naudotojams (pacientams, gydytojams - genetikams, tyrėjams).
- PA2:** Įkelti biologinius duomenis.
- PA3:** Valdyti prieigą prie asmeninių biologinių duomenų.
- PA4:** Pateikti prašymą „būti pamirštam“.

**PA5:** Sukurti paciento analizės kortelės įrašą.

**PA6:** Išsiųsti užklausą analizės atlikimui.

**PA7:** Atlikti biologinių duomenų analizę.

## 8 Funkciniai reikalavimai ir reikalavimai duomenims

### 8.1 Funkciniai reikalavimai

**PA1:** Užsiregistruoti sistemoje skirtingų kategorijų naudotojams.

<b>Tikslas/ uždavinys</b>	Valdyti asmeninius duomenimis ir naudotis sistemoje realizuotu funkcionalumu, priklausomai nuo naudotojo kategorijos.
<b>Aprašymas</b>	Realizavus šį panaudojimo atvejį skirtingos naudotojų grupės sistemoje gali atlikti skirtingus veiksmus: pacientai gali įkelti savo biologinius duomenis ir valdyti kitų asmenų prieigą prie šių duomenų; gydytojai - genetikai gali kurti pacientų analizių korteles, bet ir įkelti pacientų biologinius duomenis, teikti užklausas tyrėjams dėl biologinių duomenų analizės atlikimo, peržiūrėti analizių atlikimo statusą; tyrėjai gali vykdyti biologinių duomenų analizės ir teikti jų rezultatus gydytojams - genetikams.
<b>Prioritetas</b>	Aukštas.
<b>Užsakovo (ne)tenkinimas</b>	Netenkinimas: 5, tenkinimas: 5.
<b>Aktorius</b>	Pacientas, gydytojas - genetikas, tyrėjas.
<b>Prieš - sąlyga</b>	Sistemos naudotojas turi būti atsidaręs pradinį sistemos langą.
<b>Sužadinimo sąlyga</b>	Sistemos naudotojas atsidaro sistemos langą, kuriame pateikta asmeninės paskyros kūrimo - registracijos - forma.
<b>Pagrindinis scenarijus<sup>a</sup></b>	<ol style="list-style-type: none"><li>1. Naudotojas užpildo pateiktos asmeninės paskyros kūrimo formos laukus.</li><li>2. Naudotojas išsaugo įvestą informaciją, paspausdamas išsaugojimo mygtuką.</li><li>3. Parodomas informacinis pranešimas, informuojantis apie sėkmingai sukurtą asmeninę paskyrą.</li><li>4. Sistema prijungia naudotoją prie jo asmeninės paskyros.</li><li>5. Sistema atidaro naudotojo asmeninės paskyros langą.</li><li>6. Baigiamas PA.</li></ol>
<b>Po - sąlyga</b>	Duomenų bazėje sukuriamas naujas sistemos naudotojas, galintis prisijungti prie sistemos ir, pagal naudotojo kategoriją, naudotis sistemos funkcionalumu.
<b>Alternatyvūs scenarijai</b>	<ol style="list-style-type: none"><li>1. Naudotojas užpildo pateiktos asmeninės paskyros kūrimo formos laukus.</li><li>2. Naudotojas išsaugo įvestą informaciją, paspausdamas išsaugojimo mygtuką.</li><li>3. Parodomas informacinis pranešimas, informuojantis, kad neužpildyti visi privalomi asmeninės paskyros kūrimo formos laukai.</li><li>4. Sistema prijungia naudotoją prie jo asmeninės paskyros.</li><li>5. Sistema atidaro naudotojo asmeninės paskyros langą.</li><li>6. Baigiamas PA.</li></ol>

<sup>a</sup>Čia ir toliau žalia spalva pažymėti naudotojo veiksmai.

**PA2:** Įkelti biologinius duomenis.

<b>Tikslas/ uždavinys</b>	Pateikti biologinius duomenis, kurie gali būti panaudoti, siekiant išsiaiškinti ligų priežastis, arba moksliniais tikslais.
<b>Aprašymas</b>	Realizavus šį panaudojimo atvejį skirtingos naudotojų grupės sistemoje gali atlikti tą patį veiksmą, turint skirtingų siekių: pacientai gali įkelti savo biologinius duomenis, kurie gali būti panaudoti moksliniais tikslais, papildant biologinių duomenų saugyklą naujais genetiniais variantais; gydytojai - genetikai gali įkelti genetinius pacientų duomenis, kad jie būtų detaliau išanalizuoti tyrėjų ir būtų galima paskirti tolimesnes sutrikimo ar ligos gydymo priemonės.
<b>Prioritetas</b>	Aukštas.
<b>Užsakovo (ne)tenkinimas</b>	Netenkinimas: 5, tenkinimas: 5.
<b>Aktorius</b>	Pacientas, gydytojas - genetikas.
<b>Prieš - sąlyga</b>	Sistemos naudotojas turi būti prisijungęs prie sistemos.
<b>Sužadinimo sąlyga</b>	Sistemos naudotojas atsidaro sistemos langą, kuriame pateikta biologinių duomenų įkėlimo skiltis su metaduomenų įvedimo forma.
<b>Pagrindinis scenarijus</b>	<ol style="list-style-type: none"> <li>1. Naudotojas užpildo pateiktos duomenų įkėlimo formos laukus ir prideda biologinius duomenis saugantį failą.</li> <li>2. Naudotojas išsaugo įvestą metainformaciją bei pridėtą failą, paspausdamas išsaugojimo mygtuką.</li> <li>3. Sistema validuoja failo formatą ir turinį.</li> <li>4. Sistema užšifruoja duomenis ir išsaugo juos duomenų bazėje.</li> <li>5. Sistema įrašo metainformaciją apie įkeltą failą į blokų grandinę (taip užtikrinant duomenų nekintamumą ir veiksmų atsekamumą).</li> <li>6. Sistema priskiria įrašui identifikatorių ir susieja jį su naudotojo paskyra.</li> <li>7. Parodomas informacinis pranešimas, informuojantis apie sėkmingai įkeltus duomenis.</li> <li>8. Naudotojas peržiūri įkeltų duomenų įrašą savo paskyros skiltyje.</li> <li>9. <b>Baigiamas PA.</b></li> </ol>
<b>Po - sąlyga</b>	Į duomenų bazę įkeliami užšifruoti biologiniai duomenys.
<b>Alternatyvūs scenarijai</b>	<ol style="list-style-type: none"> <li>1. Naudotojas užpildo pateiktos duomenų įkėlimo formos laukus ir prideda biologinius duomenis saugantį failą.</li> <li>2. Naudotojas išsaugo įvestą metainformaciją bei pridėtą failą, paspausdamas išsaugojimo mygtuką.</li> <li>3. Sistema validuoja failo formatą ir turinį.</li> <li>4. Sistema nesėkmingai užšifruoja įkeltą failą dėl vidinės klaidos.</li> <li>5. Parodomas informacinis pranešimas, informuojantis, kad duomenų įkėlimas buvo nesėkmingas.</li> <li>6. Naudotojui pasiūloma pakartoti duomenų įkėlimo veiksmą.</li> <li>7. <b>Baigiamas PA.</b></li> </ol>

**PA3:** Valdyti prieigą prie asmeninių biologinių duomenų.

<b>Tikslas/ uždavinys</b>	Suteikti galimybę naudotojui (pacientui) nuspręsti, ar jo pateikti asmeniniai biologiniai duomenys gali būti prieinami kitiems naudotojams (gydytojams - genetikams ir tyrėjams). Prieigą prie asmeninių biologinių duomenų valdantis asmuo gali suteikti prieigą arba atmesti užklausą dėl duomenų prieigos.
<b>Aprašymas</b>	Realizavus šį panaudojimo atvejį skirtingos naudotojų grupės (gydytojai - genetikai, tyrėjai) gali vykdyti analizes su pateiktais biologiniais duomenimis bei daryti išvadas apie paciento sveikatos būklę. Jeigu gydytojai - genetikai arba tyrėjai netenka prieigos prie pacientų biologinių duomenų, tolimesnė duomenų analizė yra negalima.
<b>Prioritetas</b>	Aukštas.
<b>Užsakovo (ne)tenkinimas</b>	Netenkinimas: 5, tenkinimas: 5.
<b>Aktorius</b>	Pacientas.
<b>Prieš - sąlyga</b>	Sistemos naudotojas turi būti prisijungęs prie sistemos.
<b>Sužadinimo sąlyga</b>	Sistemos naudotojas atsidaro sistemos langą, kuriame realizuotas duomenų prieigos valdymo funkcionalumas.
<b>Pagrindinis scenarijus</b>	<ol style="list-style-type: none"> <li>1. Sistema pateikia paciento įkeltų biologinių duomenų sąrašą.</li> <li>2. Naudotojas pasirenka konkretų biologinių duomenų sąrašo įrašą.</li> <li>3. Sistema pateikia naudotojų, turinčių prieigą prie konkrečių biologinių duomenų, sąrašą.</li> <li>4. Naudotojas redaguoja suteiktas prieigos teises sistemos naudotojams: pratęsia prieigos laikotarpį arba atšaukia prieigą.</li> <li>5. Naudotojas suteikia naujas prieigas naujiems sistemos naudotojams.</li> <li>6. Sistema atnaukina naudotojams suteiktų prieigų sąrašą.</li> <li>7. Sistema įrašo pakeitimo informaciją į blokų grandinę.</li> <li>8. Parodomas informacinis pranešimas, informuojantis apie sėkmingai atliktą atnaujinimą.</li> <li>9. Sistema informuoja atitinkamus sistemos naudotojus apie prieigos teisių pasikeitimus.</li> <li>10. Baigiamas PA.</li> </ol>
<b>Po - sąlyga</b>	Sistemos naudotojams (gydytojams - genetikams, tyrėjams) yra suteikiama arba apribojama prieiga prie paciento biologinių duomenų.
<b>Alternatyvūs scenarijai</b>	<ol style="list-style-type: none"> <li>1. Sistema pateikia paciento įkeltų biologinių duomenų sąrašą.</li> <li>2. Naudotojas pasirenka konkretų biologinių duomenų sąrašo įrašą.</li> <li>3. Sistema pateikia naudotojų, turinčių prieigą prie konkrečių biologinių duomenų, sąrašą.</li> <li>4. Naudotojas bando redaguoti suteiktas prieigos teises konkrečiam naudotojui.</li> <li>5. Parodomas informacinis pranešimas, iformuojantis apie nesėkmingą prieigos teisių atnaujinimą (tuo atveju, jei naudotojas neaktyvus - nebedirba įstaigoje, dirbančioje su kuriama sistema).</li> <li>6. Baigiamas PA.</li> </ol>



**PA4:** Pateikti prašymą „būti pamirštam“.

<b>Tikslas/ uždavinys</b>	Leisti naudotojui (pacientui) pateikti prašymą dėl asmeninių ir įkeltų biologinių duomenų bei visų su jais susijusių įrašų panaikinimo iš saugyklų.
<b>Aprašymas</b>	Remiantis 17 BDAR straipsniu naudotojas turi galėti pateikti prašymą ištrinti visus jo pateiktus duomenis. Realizavus šį panaudojimo atvejį naudotojui iniciavus duomenų panaikinimą iš duomenų bazių yra ištrinami visi saugomi su pacientu susiję biologiniai duomenys bei su jais susiję įrašai.
<b>Prioritetas</b>	Aukštas.
<b>Užsakovo (ne)tenkinimas</b>	Netenkinimas: 3, tenkinimas: 5.
<b>Aktorius</b>	Pacientas.
<b>Prieš - sąlyga</b>	Sistemos naudotojas turi būti prisijungęs prie sistemos.
<b>Sužadinimo sąlyga</b>	Sistemos naudotojas atsidaro asmeninės paskyros peržiūros ir redagavimo sistemos langą.
<b>Pagrindinis scenarijus</b>	<ol style="list-style-type: none"> <li>1. Naudotojas asmeninės paskyros redagavimo lange pažymi parinktį „Prašymas būti pamirštam“.</li> <li>2. Sistema pateikia pasekmių, susijusių su prašymo būti pamirštam išsiuntimu, sąrašą ir nurodo, kad reikalingas naudotojo patvirtinimas.</li> <li>3. Naudotojas patvirtina, kad susipažino su pasekmėmis ir patvirtina prašymą.</li> <li>4. Sistema patikrina, ar einamuoju metu nėra atliekama paciento pateiktų biologinių duomenų analizė.</li> <li>5. Sistema panaikina naudotojo asmeninius duomenis, panaikina visų naudotojų prieigas prie biologinių duomenų, ištrina visus su naudotoju susijusius duomenis iš duomenų bazių ir užfiksuoja „pamiršimo“ įvykį blokų grandinėje.</li> <li>6. Parodomas informacinis pranešimas, informuojantis apie sėkmingai įgyvendintą prašymą būti pamirštam.</li> <li>7. Baigiamas PA.</li> </ol>
<b>Po - sąlyga</b>	Naudotojo duomenys yra pašalinti, biologiniai duomenys yra nebeprieinami kitiems sistemos naudotojams.
<b>Alternatyvūs scenarijai</b>	<ol style="list-style-type: none"> <li>1. Naudotojas asmeninės paskyros redagavimo lange pažymi parinktį „Prašymas būti pamirštam“.</li> <li>2. Sistema pateikia pasekmių, susijusių su prašymo būti pamirštam išsiuntimu, sąrašą ir nurodo, kad reikalingas naudotojo patvirtinimas.</li> <li>3. Naudotojas patvirtina, kad susipažino su pasekmėmis ir patvirtina prašymą.</li> <li>4. Sistema patikrina, ar einamuoju metu nėra atliekama paciento pateiktų biologinių duomenų analizė.</li> <li>5. Sistema nustato, kad su biologiniais duomenimis tebėra atliekami tyrimai.</li> <li>6. Parodomas informacinis pranešimas, informuojantis apie einamuoju metu negalimą prašymo būti pamirštam įgyvendinimą.</li> <li>7. Baigiamas PA.</li> </ol>

**PA5:** Sukurti paciento analizės kortelės įrašą.

<b>Tikslas/ uždavinys</b>	Leisti gydytojui - genetikui sukurti naują paciento kortelės įrašą su informacija apie analizę.
<b>Aprašymas</b>	Realizavus šį panaudojimo atvejį yra sukuriamas paciento medicininės kortelės įrašas, kuriame, esant poreikiui, užfiksuojami paciento biologiniai duomenys, pateikiami preliminarūs klinikiniai duomenys, aprašoma reikalinga analizė ir įrašomi analizės rezultatai.
<b>Prioritetas</b>	Aukštas.
<b>Užsakovo (ne)tenkinimas</b>	Netenkinimas: 5, tenkinimas: 5.
<b>Aktorius</b>	Gydytojas - genetikas.
<b>Prieš - sąlyga</b>	Sistemos naudotojas turi būti prisijungęs prie sistemos.
<b>Sužadinimo sąlyga</b>	Sistemos naudotojas atsidaro paciento kortelės įrašų kūrimo langą.
<b>Pagrindinis scenarijus</b>	<ol style="list-style-type: none"> <li>1. Naudotojas užpildo kortelės įrašo formos laukus.</li> <li>2. Naudotojas išsaugo įvestus duomenis, paspausdamas išsaugojimo mygtuką.</li> <li>3. Parodomas informacinis pranešimas, informuojantis apie sėkmingai sukurtą paciento kortelės įrašą.</li> <li>4. <b>Baigiamas PA.</b></li> </ol>
<b>Po - sąlyga</b>	Analizės užklausa yra užregistruota ir sėkmingai perduota tyrėjo vykdymui.
<b>Alternatyvūs scenarijai</b>	<ol style="list-style-type: none"> <li>1. Naudotojas užpildo kortelės įrašo formos laukus.</li> <li>2. Naudotojas išsaugo įvestus duomenis, paspausdamas išsaugojimo mygtuką.</li> <li>3. Parodomas informacinis pranešimas, informuojantis, kad neužpildyti visi privalomi kortelės įrašo kūrimo formos laukai.</li> <li>4. <b>Baigiamas PA.</b></li> </ol>

**PA6:** Išsiųsti užklausą analizės atlikimui.

<b>Tikslas/ uždavinys</b>	Leisti gydytojui - genetikui pateikti prašymą tyrėjui atlikti paciento biologinių duomenų analizę.
<b>Aprašymas</b>	Realizavus šį panaudojimo atvejį yra išsiunčiamas prašymas biologinių duomenų savininkui, kad patvirtintų, ar jis sutinka, kad jo biologiniai duomenys būtų analizuojami tyrėjo. Gavus paciento leidimą yra informuojamas tyrėjas, kad reikalingas biologinių duomenų analizės atlikimas.
<b>Prioritetas</b>	Aukštas.
<b>Užsakovo (ne)tenkinimas</b>	Netenkinimas: 5, tenkinimas: 5.
<b>Aktorius</b>	Gydytojas - genetikas.
<b>Prieš - sąlyga</b>	Sistemos naudotojas turi būti prisijungęs prie sistemos.
<b>Sužadinimo sąlyga</b>	Sistemos naudotojas atsidaro paciento kortelės įrašų kūrimo langą.
<b>Pagrindinis scenarijus</b>	<ol style="list-style-type: none"> <li>1. Naudotojas pasirenka analizės pateikimo užklausos funkciją.</li> <li>2. Sistema pateikia paciento biologinių duomenų, kuriuos galima analizuoti sąrašą.</li> <li>3. Naudotojas pasirenka aktualius biologinius duomenis bei įveda kitą su analize susijusią informaciją.</li> <li>4. Sistema pateikia tyrėjų, kurie gali atlikti analizę, sąrašą.</li> <li>5. Naudotojas pasirenka tyrėją ir išsiunčia užklausą pasirinktam tyrėjui.</li> <li>6. Sistema patikrina, ar gydytojas ir pasirinktas tyrėjas turi prieigą prie paciento duomenų.</li> <li>7. Sistema užšifruoja užklausą, išsaugo ją duomenų bazėje ir išsiunčia parinktam tyrėjui.</li> <li>8. Parodomas informacinis pranešimas, informuojantis apie sėkmingai išsiųstą užklausą.</li> <li>9. Naudotojas gali stebėti analizės atlikimo būseną.</li> <li>10. Baigiamas PA.</li> </ol>
<b>Po - sąlyga</b>	Analizės užklausa yra užregistruota ir sėkmingai perduota tyrėjo vykdymui.
<b>Alternatyvūs scenarijai</b>	<ol style="list-style-type: none"> <li>1. Naudotojas pasirenka analizės pateikimo užklausos funkciją.</li> <li>2. Sistema pateikia paciento biologinių duomenų, kuriuos galima analizuoti sąrašą.</li> <li>3. Naudotojas pasirenka aktualius biologinius duomenis bei įveda kitą su analize susijusią informaciją.</li> <li>4. Sistema pateikia tyrėjų, kurie gali atlikti analizę, sąrašą.</li> <li>5. Naudotojas pasirenka tyrėją ir išsiunčia užklausą pasirinktam tyrėjui.</li> <li>6. Sistema patikrina, ar gydytojas ir pasirinktas tyrėjas turi prieigą prie paciento duomenų.</li> <li>7. Parodomas informacinis pranešimas, informuojantis apie negalimą užklausos išsiuntimą dėl duomenų prieigos teisių neturėjimo.</li> <li>8. Baigiamas PA.</li> </ol>

**PA7:** Atlikti biologinių duomenų analizę.

<b>Tikslas/ uždavinys</b>	Išanalizuoti paciento biologinius duomenis bei pateikti įžvalgas apie juos.
<b>Aprašymas</b>	Realizavus šį panaudojimo atvejį yra įgyvendinama gydytojo - genetiko tyrėjui pateikta užklausa dėl biologinių duomenų analizės atlikimo.
<b>Prioritetas</b>	Aukštas.
<b>Užsakovo (ne)tenkinimas</b>	Netenkinimas: 5, tenkinimas: 5.
<b>Aktorius</b>	Tyrėjas.
<b>Prieš - sąlyga</b>	Sistemos naudotojas turi būti prisijungęs prie sistemos.
<b>Sužadinimo sąlyga</b>	Sistemos naudotojas atsidaro gautą analizės atlikimo užklausa.
<b>Pagrindinis scenarijus</b>	<ol style="list-style-type: none"> <li>1. Naudotojas peržiūri gautus pseudonimizuotus ir užšifruotus biologinius duomenis.</li> <li>2. Naudotojas pasirenka tinkamą analizės metodą, naudodamasis integruota arba išorine analizės vykdymo programine įranga.</li> <li>3. Naudotojas įkelia analizės rezultatus į sistemą.</li> <li>4. Sistema informuoja gydytoją - genetiką apie gautus analizės rezultatus.</li> <li>5. Sistema įrašo analizės rezultatą konkretaus paciento medicininės kortelės įrašė.</li> <li>6. Baigiamas PA.</li> </ol>
<b>Po - sąlyga</b>	Analizės užklausa yra užregistruota ir sėkmingai perduota tyrėjo vykdymui.
<b>Alternatyvūs scenarijai</b>	<ol style="list-style-type: none"> <li>1. Naudotojas peržiūri gautus pseudonimizuotus ir užšifruotus biologinius duomenis.</li> <li>2. Naudotojas pasirenka tinkamą analizės metodą, naudodamasis integruota arba išorine analizės vykdymo programine įranga.</li> <li>3. Atliekant analizę paaiškėja, kad pateikti biologiniai duomenys yra nepakankami arba netinkami, todėl gydytojo - genetiko siūsta analizės atlikimo užklausa yra atmetama, pateikiant detalias atmetimo priežastis.</li> <li>4. Baigiamas PA.</li> </ol>

## 8.2 Reikalavimai duomenims

### 8.2.1 Duomenų modelis

### 8.2.2 Duomenų modelio specifikacija

E1: Esysbė - X.

3 lentelė. Esysbės 'X' specifikacija

Atributas	Atributo apibūdinimas	Galimos reikšmės
Pacientai	Vietoje, kurioje yra sistemos svečias, gali būti silpnas arba spartus internetas.	Vietoje, kurioje yra sistemos svečias, gali būti silpnas arba spartus internetas.

## 9 Reikalavimai sistemos išvaizdai

Kuriant savarankiškos suverenios pseudonimizuotos tapatybės valdymo sistemą turi būti laikomasi šių sistemos išvaizdos reikalavimų:

**NF1: Sistemos sąsaja turi būti neįkyri.**

<b>Pagrindimas</b>	Sisteminuose languose neturi būti realizuoti iššokantys modaliniai langeliai, kuriuose reikia pasirinkti, ar tikrai norima išsaugoti įvestus duomenis.
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Užpildžius duomenų įvedimo formas ir išsaugojus duomenis nepasirodo iššokantis modalinis langelis su pranešimu apie reikalingą duomenų įvedimo patvirtinimą - duomenys yra išsaugomi be papildomo naudotojo veiksmo.
<b>Užsakovo tenkinimas</b>	1.
<b>Užsakovo netenkinimas</b>	3.
<b>Prioritetas</b>	Vidutinis.
<b>Konfliktai</b>	Nėra.

**NF2: Sistema turi būti pritaikyta darbui įvairaus amžiaus žmonėms.**

<b>Pagrindimas</b>	Sistema gali naudotis įvairaus amžiaus asmenys (sistemos svečiai, registruoti naudotojai: gydytojai - genetikai, tyrėjai), kurie dėl savo amžiaus gali turėti regėjimo sutrikimų, todėl sistemoje turi būti galima keisti langų mastelį, neišdarkant sistemos langus sudarančių elementų išdėstymo ir nepakenkiant naudotojo naudojimo sistema patirčiai.
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Sistemos naudotojai, pakeitę mastelį, gali ir toliau sėkmingai naudotis sistemos funkcionalumu ir matyti sistemos langus sudarančius elementus (nesukeliant naudotojų susierzinimo) dėl sistemos gebėjimo prisitaikyti prie keičiamo mastelio.
<b>Užsakovo tenkinimas</b>	1.
<b>Užsakovo netenkinimas</b>	3.
<b>Prioritetas</b>	Aukštas.
<b>Konfliktai</b>	Nėra.

**NF3: Sistema turi būti intuityvi.**

<b>Pagrindimas</b>	Sistema gali naudotis įvairaus amžiaus asmenys, turintys nevienodą technologinio raštingumo bei išsilavinimo lygį, todėl sistemos languose turi būti naudojami nedviprasmiški ir plačiai visuomenės asmenų daliai suprantami sistemos meniu juostos pasirinkimų pavadinimai bei turi būti panaudota kuo mažiau kompleksinių informacijos pateikimo struktūrų (pavyzdžiui, medžio struktūrų).
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Jeigu įvykdžius visų sistemos naudotojų apklausą praėjus 2 mėn. po naujos poliklinikos sistemos eksploatavimo pradžios nesulaukta daugiau nei 10% atsiliiepimų dėl sistemos neintuityvumo, nefunkcinis reikalavimas įgyvendintas.
<b>Užsakovo tenkinimas</b>	1.
<b>Užsakovo netenkinimas</b>	4.
<b>Prioritetas</b>	Aukštas.
<b>Konfliktai</b>	Nėra.

## 10 Reikalavimai panaudojamumui

Kuriant savarankiškos suverenios pseudonimizuotos tapatybės valdymo sistemą turi būti laikomasi šių panaudojamumo reikalavimų:

**NF4: Sistema turi būti nesudėtinga naudotis sistemos naudotojams.**

<b>Pagrindimas</b>	Sistema gali naudotis įvairaus amžiaus bei skirtingo išsilavinimo lygio asmenys, todėl sistemos naudotojai turi sugebėti tinkamai naudotis sistemos funkcionalumais ir užpildyti sistemoje prieinamas formas be papildomų mokymų (turi būti pateikiami detalūs funkcionalumų aprašymai; pildant sistemos formas turi būti pateikiami aiškūs ir išsamūs paaiškinimai, kokia informacija turi būti įvesta kiekviename lauke).
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Jeigu įvykdžius sistemos naudotojų apklausą praėjus 2 mėn. po naujos poliklinikos sistemos eksploatavimo pradžios nesulaukta nei vieno atsiliiepimo dėl sudėtingo sistemos naudojimo, nefunkcinis reikalavimas įgyvendintas.
<b>Užsakovo tenkinimas</b>	2.
<b>Užsakovo netenkinimas</b>	2.
<b>Prioritetas</b>	Aukštas.
<b>Konfliktai</b>	Nėra.

**NF5:** Turi būti suteikta galimybė visiems sistemos naudotojams suprasti sistemoje naudojamus terminus.

<b>Pagrindimas</b>	Sistemoje pateikta informacija turi būti parašyta taip, jog būtų suprantama ne tik medicininės dalykinės srities ekspertams. Šalia kiekvieno naudojamo medicininio termino turi būti pridėta nuoroda, nukreipianti į sistemos langą, kuriame pateiktas techninių terminų žodynas.
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Jeigu įvykdžius sistemos naudotojų apklausą praėjus 2 mėn. po naujos poliklinikos sistemos eksploatavimo pradžios nesulaukta nei vieno atsiliepimo dėl sudėtingo sistemos naudojimo, nefunkcinis reikalavimas įgyvendintas.
<b>Užsakovo tenkinimas</b>	2.
<b>Užsakovo netenkinimas</b>	2.
<b>Prioritetas</b>	Žemas.
<b>Konfliktai</b>	Nėra.

## 11 Reikalavimai vykdymo charakteristikoms

Kuriant savarankiškos suverenios pseudonimizuotos tapatybės valdymo sistemą turi būti laikomasi šių vykdymo charakteristikų reikalavimų:

**NF6:** Autentifikacijos (tapatybės patikrinimo) operacija turi būti įvykdyta per  $< 1$  s.

<b>Pagrindimas</b>	Greitas autentifikacijos procesas suteikia didesnę naudotojų patikėjimą sistema bei padeda užtikrinti po autentifikacijos sekančių operacijų atlikimą numatytu laiku.
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Jeigu pasinaudojus įrankiu Apache JMeter laiko tarpas (vidutinis atsako laikas) nuo naudotojo autentifikacijos pradžios iki patvirtinimo gavimo (fiksuoiant tapatybės būsenos pasikeitimą) neviršija 1 s, laikoma, kad nefunkcinis reikalavimas įgyvendintas.
<b>Užsakovo tenkinimas</b>	2.
<b>Užsakovo netenkinimas</b>	2.
<b>Prioritetas</b>	Žemas.
<b>Konfliktai</b>	Nėra.



NF7: Patikrinimas, ar naudotojas leido pasiekti genetinius duomenis, turi būti atliekamas per  $< 500$  ms.

<b>Pagrindimas</b>	Sistemoje pateikta informacija turi būti parašyta taip, jog būtų suprantama ne tik medicininės dalykinės srities ekspertams. Šalia kiekvieno naudojamo medicininio termino turi būti pridėta nuoroda, nukreipianti į sistemos langą, kuriame pateiktas techninių terminų žodynas.
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Jeigu įvykdžius sistemos naudotojų apklausą praėjus 2 mėn. po naujos poliklinikos sistemos eksploatavimo pradžios nesulaukta nei vieno atsiliepimo dėl sudėtingo sistemos naudojimo, nefunkcinis reikalavimas įgyvendintas.
<b>Užsakovo tenkinimas</b>	2.
<b>Užsakovo netenkinimas</b>	2.
<b>Prioritetas</b>	Žemas.
<b>Konfliktai</b>	Nėra.

## 12 Reikalavimai saugumui

NF8: Visi saugomi genetiniai duomenys turi būti šifruojami.

<b>Pagrindimas</b>	....
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Jeigu testuojant šifravimą realiuoju laiku, naudojant tinklo analizatorius, asmeninių duomenų negalima perskaityti, laikoma, kad nefunkcinis reikalavimas įgyvendintas.
<b>Užsakovo tenkinimas</b>	2.
<b>Užsakovo netenkinimas</b>	2.
<b>Prioritetas</b>	Žemas.
<b>Konfliktai</b>	Nėra.

NF9: Naudotojų identifikavimo duomenys turi būti atskirti nuo genetinių duomenų, naudojant pseudonimizaciją ir anonimizaciją.

<b>Pagrindimas</b>	Sistemos pažeidimo atveju turi būti užtikrintas genetinių duomenų, galinčių atskleisti ne tik asmens, bet ir jo šeimos narių asmeninę informaciją, konfidencialumas, siekiant išvengti teisės pažeidimų.
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	....
<b>Užsakovo tenkinimas</b>	5.
<b>Užsakovo netenkinimas</b>	5.
<b>Prioritetas</b>	Aukštas.
<b>Konfliktai</b>	Nėra.

## 13 Teisiniai reikalavimai

NF10: Sistemoje turi būti laikomasi BDAR reikalavimo dėl pacientų duomenų pseudonimizavimo.

<b>Pagrindimas</b>	Sistemos, kuriose vykdomas asmenų biologinių duomenų saugojimas bei apdorojimas, turi atitikti BDAR 32 straipsnyje aprašytą reikalavimą, nurodantį, tvarkant asmens duomenis turi būti naudojamos tinkamos techninės ir organizacinės priemonės, įskaitant pseudonimizavimą, siekiant užtikrinti duomenų saugumą.
<b>Šaltinis</b>	Užsakovas.
<b>Atitikimo kriterijus</b>	Laikoma, kad nefunkcinis reikalavimas įgyvendintas, jeigu atlikus sistemos duomenų bazės struktūros analizę nenustatomas genetinių duomenų saugojimas kartu su identifikavimo duomenimis bei testavimo metu nenustatyti tiesiogiai identifikuojantys asmeniniai duomenys.
<b>Užsakovo tenkinimas</b>	5.
<b>Užsakovo netenkinimas</b>	5.
<b>Prioritetas</b>	Aukštas.
<b>Konfliktai</b>	Nėra.

## 14 Naujos problemos

14.1 Problemos diegimo palinkai

14.2 Įtaka jau instaliuotoms sistemoms

14.3 Neigiamas vartotojų nusiteikimas

14.4 Kliudantys diegimo aplinkos apribojimai

14.5 Galimos naujos sistemos sukeltos problemos

## 15 Uždaviniai

### 15.1 Sistemos pateikimo žingsniai (etapai)

### 15.2 Vystymo etapai

## 16 Rizikos ir jų valdymas

**R1:** Pakeisti ar sugadinti biologiniai duomenys gali lemti neteisingą analizę.

<b>Valdymas</b>	Biologinius duomenis integruoti į blokų grandinę, siekiant užtikrinti duomenų nekintamumą.
<b>Tikimybė</b>	Žema.
<b>Poveikis</b>	Aukštas.

**R2:** Nepaisant pseudonimizavimo, biologiniai duomenys gali būti susieti su konkrečiais asmenimis.

<b>Valdymas</b>	Griežtai riboti prieigos teisės pagal naudotojo kategoriją ir vykdyti duomenų pseudonimų keitimą.
<b>Tikimybė</b>	Žema.
<b>Poveikis</b>	Aukštas.

**R3:** Sistemoje realizuotas funkcionalumas gali neatitikti asmens duomenų apsaugos reikalavimų.

<b>Valdymas</b>	Skirti ypatingą dėmesį BDAR reglamento analizei ir atitinkamam sistemos pritaikymui.
<b>Tikimybė</b>	Žema.
<b>Poveikis</b>	Aukštas.

**R4:** Dėl sistemos gedimo ar neteisingo atsarginio kopijavimo gali būti prarasti duomenys.

<b>Valdymas</b>	Vykdyti reguliarių duomenų atsarginių kopijų kūrimą, aiškiai dokumentuoti duomenų atstatymo procesą bei periodiškai vykdyti šio proceso testavimą.
<b>Tikimybė</b>	Žema.
<b>Poveikis</b>	Aukštas.

**R5:** Sistemos veikimo sutrikimai, galintys kilti po sistemos diegimo į užsakovo aplinkas.

<b>Valdymas</b>	Pradėti vykdyti sistemos testavimą ankstyvosiose sistemos vystymo stadijose, siekiant ištestuoti visą sistemos funkcionalumą, bei turėti aiškiai dokumentuotą sistemos diegimo planą, kuriame būtų detalios aprašyti ir veiksmai, kurių reikia imtis nesėkmingo diegimo atveju.
<b>Tikimybė</b>	Aukšta.
<b>Poveikis</b>	Aukštas.

**R6:** Dėl nenumatytų priežasčių gali vėluoti projektas - sistema gali būti sudiegta vėliau nei yra numatyta projekto plane.

<b>Valdymas</b>	Pradėti vykdyti sistemos testavimą ankstyvosiose sistemos vystymo stadijose, siekiant identifikuoti klaidas kuo anksčiau, bei organizuoti reguliarius susitikimus su užsakovu, kad būtų aptartas darbų progresas bei iškilę sunkumai.
<b>Tikimybė</b>	Aukštas.
<b>Poveikis</b>	Aukštas.

## 17 Kaina

## 18 Naudotojo dokumentacija

Žemiau yra pateiktas naudotojams aktualios dokumentacijos aprašymas.

<b>Pavadinimas</b>	Sistemos naudojimo vadovas.
<b>Atsakingas asmuo</b>	Danielė Stasiūnaitė.
<b>Naudotojų įtraukimas į dokumentacijos ruošimą</b>	Tiesioginių sistemos naudotojų įtraukimas į naudotojo vadovo kūrimą yra nenumatytas.
<b>Dokumento atnaujinimas</b>	Jeigu po pagrindinio sistemos diegimo tebėra atliekami reguliarūs sistemos vystymo ir tobulinimo darbai, naudojimo vadovas turi būti atnaujinamas ir perduodamas užsakovui kas 2 mėnesius. Kitu atveju, naudojimo vadovas atnaujinamas tik atskiru užsakovo prašymu.
<b>Dokumento pateikimo forma ir turinys</b>	Sistemos naudojimo vadovas turi būti prieinamas pradiname sistemos lange kaip atskiras atsisiunčiamas PDF dokumentas. Vadove turi būti pateiktas sistemos pavadinimas, dokumento versija, rengimo data, atsakingas asmuo, sistemos paskirtis bei turi būti aprašytos visos sistemoje realizuotos funkcijos.