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

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.

Mobilusis telefonas:	+37066428763.
El. pašto adresas	mindaugas.vasiljevas@ktu.lt.
Adresas	XI rūmai 3C2b korpusas.
Informacijos galima teirautis	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

- **Funkcijos:** Valdyti savo asmeninių genetinių duomenų prieinamumą kitoms naudotojų grupėms; esant poreikiui, įkelti genetinius duomenis; peržiūrėti analizių, atliktų su genetiniais duomenimis, rezultatus.
- **Patirtis dalykinėje srityje:** Žema.
- **Patirtis IT srityje:** Žema.
- **Papildomos charakteristikos:** 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).
- **Prioritetas:** Aukštas.

Gydytojai - genetikai

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

Tyrėjai

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

Pacientai

- Vietoje, kurioje yra sistemos svečias, gali būti silpnas arba spartus internetas.

Gydytojai - genetikai

- Asmenys naudojasi sistema gerai apšviestuose vieno asmens kabinetuose, leidžiančių užtikrinti pacientų konfidencialumą konsutlacijų metu.
- Kabinetuose kompiuteriai išdėstyti taip, kad pacientai negali matyti gydytojo kompiuterio ekrano.
- Kabinetuose užtikrintas spartus internetas.

Tyrėjai

- Asmenys naudojasi sistema gerai apšviestuose kelių asmenų kabinetuose.
- Kabinetuose tyrėjų darbastaliai su kompiuteriais yra išdėstyti taip, kad darbuotojai nemato vienas kito kompiuterių.

- Aplinkoje užtikrintas spartus internetas.
- Kabinetai turi ribotą fizinę prieigą - yra įdiegta kortelinė durų kontrolės sistema.

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

7.2 Panaudojimo atvejų sąrašas

1. Užsiregistruoti sistemoje skirtingų kategorijų naudotojams (pacientams, gydytojams - genetikams, tyrėjams).
2. Įkelti biologinius duomenis.
3. Valdyti prieigą prie asmeninių biologinių duomenų.
4. Pateikti prašymą „būti pamirštam“.
5. Išsiųsti užklausą analizės atlikimui.
6. Sukurti paciento analizės kortelę.
7. Peržiūrėti pacientų analizių atlikimo būseną.
8. Atlikti biologinių duomenų analizę.
9. Pateikti analizės rezultatus.

8 Funkciniai reikalavimai ir reikalavimai duomenims

8.1 Funkciniai reikalavimai

8.2 Reikalavimai duomenims

9 Reikalavimai sistemos išvaizdai

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

NF1: Sistemos sąsaja turi būti neįkyri.

Pagrindimas	Sisteminiuose languose neturi būti realizuoti iššokantys modaliniai langeliai, kuriuose reikia pasirinkti, ar tikrai norima išsaugoti įvestus duomenis.
Šaltinis	Užsakovas.
Atitikimo kriterijus	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.
Užsakovo tenkinimas	1.
Užsakovo netenkinimas	3.
Prioritetas	Vidutinis.
Konfliktai	Nėra.

NF2: Sistema turi būti pritaikyta darbui įvairaus amžiaus žmonėms.

Pagrindimas	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.
Šaltinis	Užsakovas.
Atitikimo kriterijus	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.
Užsakovo tenkinimas	1.
Užsakovo netenkinimas	3.
Prioritetas	Aukštas.
Konfliktai	Nėra.

NF3: Sistema turi būti intuityvi.

Pagrindimas	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).
Šaltinis	Užsakovas.
Atitikimo kriterijus	Jeigu įvykdžius visų sistemos naudotojų apklausą praėjus 2 mėn. po naujos poliklinikos sistemos eksploatavimo pradžios nesulaukta daugiau nei 10% atsiliepimų dėl sistemos neintuityvumo, nefunkcinis reikalavimas įgyvendintas.
Užsakovo tenkinimas	1.
Užsakovo netenkinimas	4.
Prioritetas	Aukštas.
Konfliktai	Nėra.

10 Reikalavimai panaudojamumui

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

NF4: Sistema turi būti nesudėtinga naudotis sistemos naudotojams.

Pagrindimas	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).
Šaltinis	Užsakovas.
Atitikimo kriterijus	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.
Užsakovo tenkinimas	2.
Užsakovo netenkinimas	2.
Prioritetas	Aukštas.
Konfliktai	Nėra.

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

Pagrindimas	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.
Šaltinis	Užsakovas.
Atitikimo kriterijus	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.
Užsakovo tenkinimas	2.
Užsakovo netenkinimas	2.
Prioritetas	Žemas.
Konfliktai	Nėra.

11 Reikalavimai vykdymo charakteristikoms

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

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

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

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

Pagrindimas	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.
Šaltinis	Užsakovas.
Atitikimo kriterijus	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.
Užsakovo tenkinimas	2.
Užsakovo netenkinimas	2.
Prioritetas	Žemas.
Konfliktai	Nėra.

12 Reikalavimai saugumui

NF8: Visi saugomi genetiniai duomenys turi būti šifruojami.

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

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

Pagrindimas	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.
Šaltinis	Užsakovas.
Atitikimo kriterijus	....
Užsakovo tenkinimas	5.
Užsakovo netenkinimas	5.
Prioritetas	Aukštas.
Konfliktai	Nėra.

13 Teisiniai reikalavimai

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

Pagrindimas	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.
Šaltinis	Užsakovas.
Atitikimo kriterijus	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.
Užsakovo tenkinimas	5.
Užsakovo netenkinimas	5.
Prioritetas	Aukštas.
Konfliktai	Nėra.

14 Atviri klausimai (problemos)

15 Naujos problemos

15.1 Problemos diegimo palinkai

15.2 Įtaka jau instaliuotoms sistemoms

15.3 Neigiamas vartotojų nusiteikimas

15.4 Kliudantys diegimo aplinkos apribojimai

15.5 Galimos naujos sistemos sukeltos problemos

16 Uždaviniai

16.1 Sistemos pateikimo žingsniai (etapai)

16.2 Vystymo etapai

17 Uždaviniai

17.1 Pritaikymas (Cutover)

17.2 Reikalavimai esamų duomenų perkėlimui

17.3 Reikalingas duomenų transformavimas perkeliant į naują sistemą

18 Rizikos

18.1 Galimos sistemos kūrimo rizikos

18.2 Atsitiktinumų (rizikų) valdymo planas

19 Kaina

20 Naudotojo dokumentacija ir apmokymas