**VIISP AUTENTIFIKAVIMO POSISTEMĖS SUKŪRIMO, MODERNIZAVIMO IR DIEGIMO PASLAUGŲ TECHNINĖ SPECIFIKACIJA**

Versija 1.02, 2024-11-13

Turinys

[I SKYRIUS: BENDRA INFORMACIJA 1](#_Toc1818014646)

[II SKYRIUS: ESAMOS SITUACIJOS IR PROBLEMATIKOS APRAŠYMAS 2](#_Toc2111298822)

[III SKYRIUS: BENDRI REIKALAVIMAI PERKAMOMS PASLAUGOMS 3](#_Toc276154382)

[IV SKYRIUS: PRINCIPINĖ DABARTINĖS TNP SCHEMA 3](#_Toc405431880)

[V SKYRIUS: AUTENTIFIKAVIMO IR ATSTOVAVIMO NUSTATYMO PROCESAS 4](#_Toc776042178)

[VI SKYRIUS: REIKALAVIMAI AUTENTIFIKAVIMO POSISTEMEI 8](#_Toc96192203)

[VI.1. Reikalavimai suderinamumui 8](#_Toc1939717109)

[VI.2 Reikalavimai programinės įrangos architektūrai 8](#_Toc370490352)

[VI.3 Reikalavimai naudotojo sąsajai 16](#_Toc87523003)

[VI.4 Integracijos su išorinėmis autentifikavimo sistemomis 17](#_Toc318549970)

[VI.5. Reikalavimai autentifikavimo ir saugos standartų palaikymui 18](#_Toc541375494)

[VI.6. Reikalavimai audito žurnalams ir jų valdymui 18](#_Toc532370113)

[VI.7. Reikalavimai stebėsenos galimybėms 19](#_Toc832174641)

[VI.8. Reikalavimai integracijoms 20](#_Toc1479498366)

[VI.9 Reikalavimai duomenų ir konfigūracijos migravimui 20](#_Toc1319051183)

[VI.10 Reikalavimai VIISP modifikavimui 20](#_Toc2119612209)

[VI.11 Reikalavimai diegimui 20](#_Toc160349347)

[VII SKYRIUS: REIKALAVIMAI PASLAUGŲ TEIKIMUI 21](#_Toc548552787)

[VII.1 Reikalavimai įgyvendinimo būdui ir paslaugų teikimo etapams 21](#_Toc1169890981)

[VII.2 Reikalavimai išeities kodo ir darbų valdymui 26](#_Toc577279437)

[VII.3. Reikalavimai dokumentacijai 27](#_Toc1091233085)

[VII.5 Reikalavimai priėmimo testavimui 27](#_Toc853148341)

[VII.6 Reikalavimai garantinės priežiūros ir palaikymo paslaugoms 28](#_Toc1527911450)

[VII SKYRIUS: PRIEDAI 28](#_Toc29339570)

# I SKYRIUS: BENDRA INFORMACIJA

1. Apie projektą - Valstybės skaitmeninių sprendimų agentūra (toliau – Perkančioji organizacija,PO, VSAA) kartu su partneriais valstybės įmone Registrų centru, Nacionaline švietimo agentūra, Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos įgyvendina projektą Nr. 02-088-P-0006 „SKAITMENINIŲ PASLAUGŲ PLATFORMA“ pagal 2021–2030 metų plėtros programos valdytojos Ekonomikos ir inovacijų ministerijos valstybės skaitmeninimo plėtros programos pažangos priemonę Nr. 05-002-01-07-08 „Kurti technologinius sprendimus ir įrankius, leidžiančius saugiai ir patogiai naudotis paslaugomis“. Projektas finansuojamas 2021‒2027 metų Ekonomikos gaivinimo ir atsparumo didinimo priemonės ir Lietuvos Respublikos valstybės biudžeto lėšomis. Projekto metu bus sukurta Skaitmeninių paslaugų platforma (SPP), kurioje greitai, lengvai ir patogiai bus kuriamos į naudotoją orientuotos skaitmeninės paslaugos nustatytais standartizuotais įrankiais ir metodikomis. SPP bus realizuotas standartizuotas duomenų apsikeitimas ir valdymas tarp institucijų per API sistemą, užtikrinančią pakartotinį duomenų panaudojimą, paslaugų sąveikumą ir duomenų vientisumą, modernizuota asmens atpažinties paslauga, realizuota atsižvelgiant eIDAS ("Electronic IDentification, Authentication and trust Services", eIDAS yra elektroninės atpažinties priemonė ir elektroninių operacijų patikimumo užtikrinimo paslaugą Europos Sąjungoje) reglamento pakeitimuose išplėstą paslaugų apimtį, modernizuota paslaugų konstravimo paslauga ir kiti bendro naudojimo funkcionalumai, kurie užtikrins patogų ir greitą paslaugų ir viešojo valdymo procedūrų skaitmenizavimą. Taip pat, SPP apimtyje bus realizuoti Europos Komisijos bendrųjų skaitmeninių vartų vienkartinio duomenų pateikimo techninės sistemos (angl. Single Digital Gateway Once-Only Technical System) (toliau – SDG OOTS) reikalavimai, kurie užtikrins principo „tik vieną kartą“ taikymą teikiant skaitmenines paslaugas ES piliečiams ir įgalins tarpvalstybinius duomenų mainus naudojant saugų eDelivery mazgų tinklą. Įgyvendinant SPP projektą bus sukurtas nacionalinis OOTS bendro naudojimo integracinis komponentas, skirtas administracinių paslaugų teikimui reikalingų registrinių duomenų gavimui ir teikimui tarp ES viešojo administravimo institucijų, bus integruotas į SDG paslaugų užsakymo formas ir leis ES piliečiui realiu laiku gauti bei pateikti įrodymus, kurių reikia el. paslaugos suteikimui iš ES viešojo administravimo institucijų. Visos SDG paslaugos, kurios yra teikiamos nacionalinių paslaugų teikėjų, bus pritaikytos ir prieinamos ES piliečiams.
2. **Pirkimo tikslas** – atskirti ir modernizuoti autentifikavimo komponentą, naudojamą [epaslaugos.lt](http://www.epaslaugos.lt) portale į nepriklausomai kitos nuo el. paslaugų platformos technologijų ir/ar versijų diegiamą, valdomą, vystomą ir palaikomą posistemę, siekiant:
   1. pagerinti Tapatybės nustatymo paslaugos patikimumą, našumą atsparumą ribinėms apkrovoms,
   2. užtikrinti autentifikavimo paslaugos nepertraukiamą teikimą pereinamuoju laikotarpiu, kuriant naują SPP, ir vėliau,
   3. užtikrinti tęstinį efektyvų ir tvarų Valstybės informacinių išteklių sąveikumo platformos (toliau - VIISP) veikimą.
3. **Pirkimo objektas**:
   1. VIISP autentifikavimo posistemės sukūrimo, modernizavimo ir diegimo paslaugos (toliau – AP sukūrimo, modernizavimo ir diegimo paslaugos),
   2. VIISP autentifikavimo posistemės garantinės priežiūros ir palaikymo paslaugos (toliau – Palaikymo paslaugos, Priežiūros ir palaikymo paslaugos).

**Paslaugos neturi kelti grėsmės nacionaliniam saugumui, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 8 ir 9 dalies nuostatomis.**

1. Pasirašius Sutartį per 10 (dešimt) darbo dienų nuo Sutarties įsigaliojimo dienos bus pasirašomas konfidencialumo pasižadėjimas. Taip pat, jeigu bus poreikis, bus pasirašomas Asmens duomenų tvarkymo susitarimas per 20 (dvidešimt) darbo dienų nuo Sutarties įsigaliojimo dienos.
2. Vadovaujantis Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 ,,Dėl aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“ (aktuali redakcija 2022 m. gruodžio 13 d. įsakymas Nr. D1-401) 4 punktu, Pirkimas laikomas žaliuoju, nes tenkina 4.4.3 papunktyje nustatytą sąlygą, t. y. perkama tik nematerialaus pobūdžio (intelektinė) paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos. Papildomi aplinkos apsaugos kriterijai nustatomi Sutarties specialiose sąlygose.

# II SKYRIUS: ESAMOS SITUACIJOS IR PROBLEMATIKOS APRAŠYMAS

1. Perkančioji organizacija vysto ir prižiūri www.epaslaugos.lt portalą (toliau – Portalas) bei jo sudėtinius modulius, teikia technines priemones bei metodines rekomendacijas el. paslaugų konstravimui bei įdiegimui Portale, teikia priemones institucijoms publikuoti informaciją apie viešąsias paslaugas Portale, užtikrina sąsajas su el. paslaugas teikiančiomis kitomis informacinėmis sistemomis bei pateikia bendrojo naudojimo komponentus, skirtus lengvesniam funkcijų sukūrimui kitų institucijų informacinėse sistemose (naudotojų identifikavimo, mokėjimų, sutarčių valdymo, duomenų mainų bei kitus). Tame tarpe viena iš populiariausių Portalo paslaugų yra Tapatybės nustatymo paslauga (toliau – TNP).
   1. TNP aprašymas skirtas institucijoms ir jų tiekėjams: <https://www.epaslaugos.lt/portal/content/1257>.
   2. TNP teikimo pradinis Portalo langas naudotojams: <https://www.epaslaugos.lt/portal/nlogin>.
2. Problemos ir tobulintinos vietos:
   1. Šiuo metu TNP yra integrali VIISP sudarančios programinės įrangos dalis, kartu su kitomis specializuotomis el. paslaugomis savo veikimui naudojanti bendrą VIISP kodo bazę, sisteminę programinę įrangą ir infrastruktūros resursus. Tuo tarpu, TMP dažniau už kitas el. paslaugas naudojama kitų įstaigų informacinių sistemų naudotojų tapatybės nustatymui, kas sudaro ribinius apkrovimus, nesusijusius su pagrindiniu VIISP programinės įrangos funkcionalumu. Dabartinė VIISP architektūra nenumato galimybės atskirai valdyti resursus, dedikuotus TNP pasiekiamumo, našumo ir atsparumo užtikrinimui.
   2. TNP, pilnai integruota į esamą VIISP programinę įrangą, apriboja ir kelia rizikas dabartinės epaslaugos.lt versijai pakopinei transformacijai į kuriamos naują skaitmeninių paslaugų platformos versiją.
   3. Dabartinė TNP versija ir sąsajų techninės galimybės nepilnai atitinka teisės akto - Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. kovo 25 d. įsakymo Nr. T-36 „Dėl Duomenų teikimo formatų ir standartų rekomendacijų patvirtinimo“ (<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2ffb8e70cda011ed9b3c9397e1236c2a?positionInSearchResults=0&searchModelUUID=c5b6937d-5159-48c5-95c2-e6961dbb6be5>) reikalavimus dėl duomenų mainų sąsajų (OpenAPI v3, REST API), autentifikavimo ir saugos standartų (OAuth v2, SAML) ir kt.

# III SKYRIUS: BENDRI REIKALAVIMAI PERKAMOMS PASLAUGOMS

1. VIISP Autentifikavimo posistemės (toliau – AP) sukūrimo, modernizavimo ir diegimo paslaugas sudaro:
   1. AP sukūrimas, atskiriant jos funkcionalumą, diegimą, priežiūrą ir gyvavimo ciklo valdymą nuo esamos pagrindinės VIISP programinės įrangos taip, kad AP būtų galima diegti ir eksploatuoti nepriklausomai nuo likusios VIISP.
   2. AP integravimas į Reglamento (ES) Nr. 910/2014 reikalavimus atitinkančią eIDAS elektroninės atpažinties priemonę, užtikrinančią tarpvalstybinių elektroninių paslaugų teikimą;
   3. AP integracinių programinių sąsajų ir palaikomų saugos standartų modernizavimas pagal teisės akto - Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. kovo 25 d. įsakymo Nr. T-36 „Dėl Duomenų teikimo formatų ir standartų rekomendacijų patvirtinimo“ (<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2ffb8e70cda011ed9b3c9397e1236c2a?positionInSearchResults=0&searchModelUUID=c5b6937d-5159-48c5-95c2-e6961dbb6be5>) reikalavimus.
   4. AP diegimas ir parengimas gamybinei eksploatacijai.
   5. AP gamybinės eksploatacijos priežiūra.
   6. AP administravimo metodinės medžiagos parengimas.
   7. Sąveikumo su AP metodinės medžiagos, skirtos institucijoms ir jų tiekėjams, parengimas.

# IV SKYRIUS: PRINCIPINĖ DABARTINĖS TNP SCHEMA

1. Žemiau pateikiama esama principinė VIISP TNP ir išorinių institucijų informacinių sistemų sąveikos bei ir naudotojo veiksmų eiga, kuri turi būti išlaikyta ir atskiriamoje AP:
   1. Naudotojas per epaslaugos.lt prisijungia prie portalo; (1-A - alternatyvus prisijungimas, kai prisijungimas inicijuojamas iš išorinės sistemos);
   2. Naudotojas epaslaugos.lt portale pasirenka vieną iš atstovavimų;
   3. Atstovavimas pagal įstatymą tikrinamas išoriniuose registruose; Šiuo metu nėra veikiančių neveiksnių ir Įgaliojimų registro sąsajų;
   4. Naudotojas portale pasirenka vieną iš publikuojamų paslaugų;
   5. Naudotojui rodomas sutikimo perduoti duomenis išorinei sistemai langas su konkrečiais duomenimis, kurie bus perduodami;
   6. Duomenų paketas perduodamas į išorinę sistemą;
   7. Prisijungimo metu paslauga naudoja tiek vidines, tiek išorines integracijas paslaugos konfigūracijai nustatyti. Paslaugos konfigūracija remiasi:
      1. Techniniai paslaugos teikimo nustatymai (SSL sertifikatai, adresai, paketo formavimo nustatymai);
      2. Su konkrečia el. paslauga, kuriai atliekamas identifikavimas, susiję nustatymai - leidžiami prisijungimo būdai, atstovavimai, ribojimai (pagal naudotojus, IP adresus);
      3. Išorinių registrų teikiama informacija apie naudotoją tapatybės patikrinimui:
         1. Gyventojų registro (GR),
         2. Juridinių asmenų registro (JAR),
         3. Valstybės tarnautojų registro (VATAR),
         4. Migracijos departamento informacinės sistemos (MIGRIS).
      4. Išorinių registrų teikiama informacija apie galimus atstovauti asmenis
         1. Juridinių asmenų registro (JAR),
         2. Registrų centro Įgaliojimų registro (ĮR),
         3. Registrų centro Neveiksnių ir ribotai veiksnių asmenų registras (NR),
         4. Valstybės tarnautojų registro (VATAR).

A diagram of a system

Description automatically generated

pav. 1 Sąveikos su TNP schema

# V SKYRIUS: AUTENTIFIKAVIMO IR ATSTOVAVIMO NUSTATYMO PROCESAS

1. Procesų dalyviai
   1. Naudotojai:
      1. LR Fizinis asmuo (LR FA),
      2. fizinis asmuo užsienio pilietis (FAU),
      3. Juridinis asmuo, juridinio asmens atstovas (JA),
      4. Valstybės tarnautojas, pareigūnas (VT).
   2. Institucijų informacinės sistemos:
      1. Bet kokia institucijos ar įmonės informacinė sistema, kurios autentifikavimo mechanizmas integruotas su Valdžios vartais,
      2. Perspektyvoje - VIISP.
   3. Tapatybės nustatymo sistemos
      1. Bankai:
         1. Swedbank, SEB, Luminor, Citadele, Šiaulių bankas, URBO, LKU Kredito unijų grupė, KREDA jungtinės kredito unijos, RATO, Paysera,
      2. eIDAS,
      3. Elektroninio parašo tikrinimo sistemos, tarpininkaujant Dokobit,
      4. Išmaniųjų tapatybės kortelių skaitytuvų komponentai ir el. parašo tikrinimo sistemos, tarpininkaujant Dokobit,
      5. Nekontaktinės asmens tapatybės kortelės tikrinimo sistema Softemia mCard LT.
2. Proceso eigoje naudojami išoriniai ir vidiniai registrai:
   1. Autentifikuoto naudotojo tapatybės duomenų tikrinimo registrai:
      1. Gyventojų registras (GR),
      2. Juridinių asmenų registras (JAR),
      3. Valstybės tarnautojų registras (VATAR),
      4. Migracijos departamento informacinės sistema (MIGRIS).
   2. Autentifikuoto naudotojo atstovavimo kitiems asmenims nustatymo registrai:
      1. Registrų centro Įgaliojimų registras (ĮR),
      2. Registrų centro Neveiksnių ir ribotai veiksnių asmenų registras (NR),
      3. Juridinių asmenų registras (JAR).
3. Apibendrintas autentifikavimo ir atstovavimo procesas pateiktas diagramoje kitame puslapyje:

A diagram of a diagram

Description automatically generated

**pav. 2 Autentifikavimo ir atstovavimo nustatymo procesas**

1. Procesas gali būti inicijuotas naudotojui prisijungus prie AP tiesiogiai arba per išorinės institucijos informacinę sistemą (toliau – Institucijos IS).
2. Jeigu prisijungimas prie AP inicijuojamas iš Institucijos IS, Institucijos IS kreipiasi į AP perduodama atitinkamą duomenų paketą (žr. <https://www.epaslaugos.lt/portal/content/1257>).
   1. Kaip ir aprašyta TNP specifikacijoje, Institucijos IS gali nurodyti, tapatybės atributai ir papildomi naudotojo duomenys turėtų būti gražinami kartu su tapatybės duomenų rinkiniu, pavyzdžiui, ar galimas atstovavimo pasirinkimas, kokia kalba (en, lt) atvaizduoti tapatybės nustatymo ekranvaizdžius, kuriuo adresu grąžinti naudotoją sėkmingo tapatybės nustatymo atveju, koreliaciniai duomenys, kurie bus grąžinti atgal į Institucijos IS be pakeitimų.
   2. Institucijos IS taip pat gali nurodyti/apriboti, kokio tipo naudotojai gali jungtis prie sistemos (gyventojai, juridiniai asmenys, valstybės tarnautojai), kokiomis autentifikacijos priemonėmis naudotojui bus leidžiama nustatyti tapatybę.
   3. Institucijos IS duomenų paketo nustatymai gali reguliuoti, ar naudotojas privalo peržiūrėti ir patvirtinti savo tapatybės ir atstovavimo duomenis, prieš perduodant juos Institucijos IS, ar tai turi įvykti automatiškai.
3. AP vykdo autentifikavimą - tapatybės nustatymą per išorines tapatybių nustatymo sistemas.
4. Gavus autentifikuoto naudotojo tapatybę AP vykdo tapatybės patikrą per tapatybės tikrinimo registrus.
5. Jeigu tai leidžiama Institucijos IS perduotuose nustatymuose ir/ar pasirinkus naudotojui, autentifikuotas naudotojas turi turėti galimybę pasirinkti teisėtą atstovavimą kitam asmeniui. Šiam tikslui AP nustato galimus atstovavimui asmenis pagal atstovavimo kitiems asmenims nustatymo registrus.
   1. Tuo atveju, kai kito asmens atstovavimas leidžiamas, AP atvaizduoja visus galimus atstovauti asmenis pagal atstovavimo registrų duomenis, galimai filtruojant pagal Institucijos IS perduotus nustatymus.
   2. Tuo atveju, jeigu asmuo turi atstovavimo įgaliojimus, tačiau Institucijos IS perduotuose nustatymuose atstovavimas kitam asmeniui uždraustas, atstovavimo variantai rodomi neaktyvuoti (angl. disabled) su paaiškinančia kontekstine pagalba.
6. Klaidos atveju bet kokiame proceso žingsnyje naudotojas informuojamas apie klaidą ir AP pasiūlo pakartoti veiksmą, jeigu tai leidžiama nustatymuose. Naudotojui atsisakius arba neturint techninės galimybės tęsti procesą naudotojas turi būti grąžinamas į AP proceso pradžią su atitinkamu pranešimu.
7. Įvykus klaidai bet kokiame proceso žingsnyje (nenustačius tapatybės, nepraėjus tapatybės patikros, vykdant paiešką atstovavimo registruose) rodomas informacinis pranešimas su galimybe pakartotinai pasirinkti autentifikavimo būdą, pakartoti veiksmą, grįžti į AP proceso pradžią arba į Institucijos IS be autentifikacijos.
8. Jeigu taip nurodyta Institucijos IS perduotuose ir/ar AP nustatymuose sėkmingai nustačius tapatybę ir galimai pasirinkus atstovavimą naudotojas turi peržiūrėti ir patvirtinti išorinei informacinei sistemai perduodamus duomenis. Atsisakius, naudotojas grąžinamas į AP proceso pradžią.
9. Sėkmingo tapatybės nustatymo, patikros ir galimo atstovavimo pasirinkimo atveju,
   1. jeigu prisijungimas prie AP buvo inicijuotas Institucijos IS, sėkmingo tapatybės ir galimo atstovavimo nustatymo atveju AP nukreipia naudotoją bei perduoda kitus duomenis procesą inicijavusiai Institucijos IS, užtikrinant vieningo autentifikavimo (angl. Single Sign On, SSO) mechanizmą.
   2. jeigu prisijungimas prie AP inicijuojamas naudotojo tiesiogiai, tuomet sėkmingai atlikus tapatybės ir galimo atstovavimo nustatymą, AP nukreipia naudotoją į [www.epaslaugos.lt](http://www.epaslaugos.lt) naudojant tą patį SSO mechanizmą.

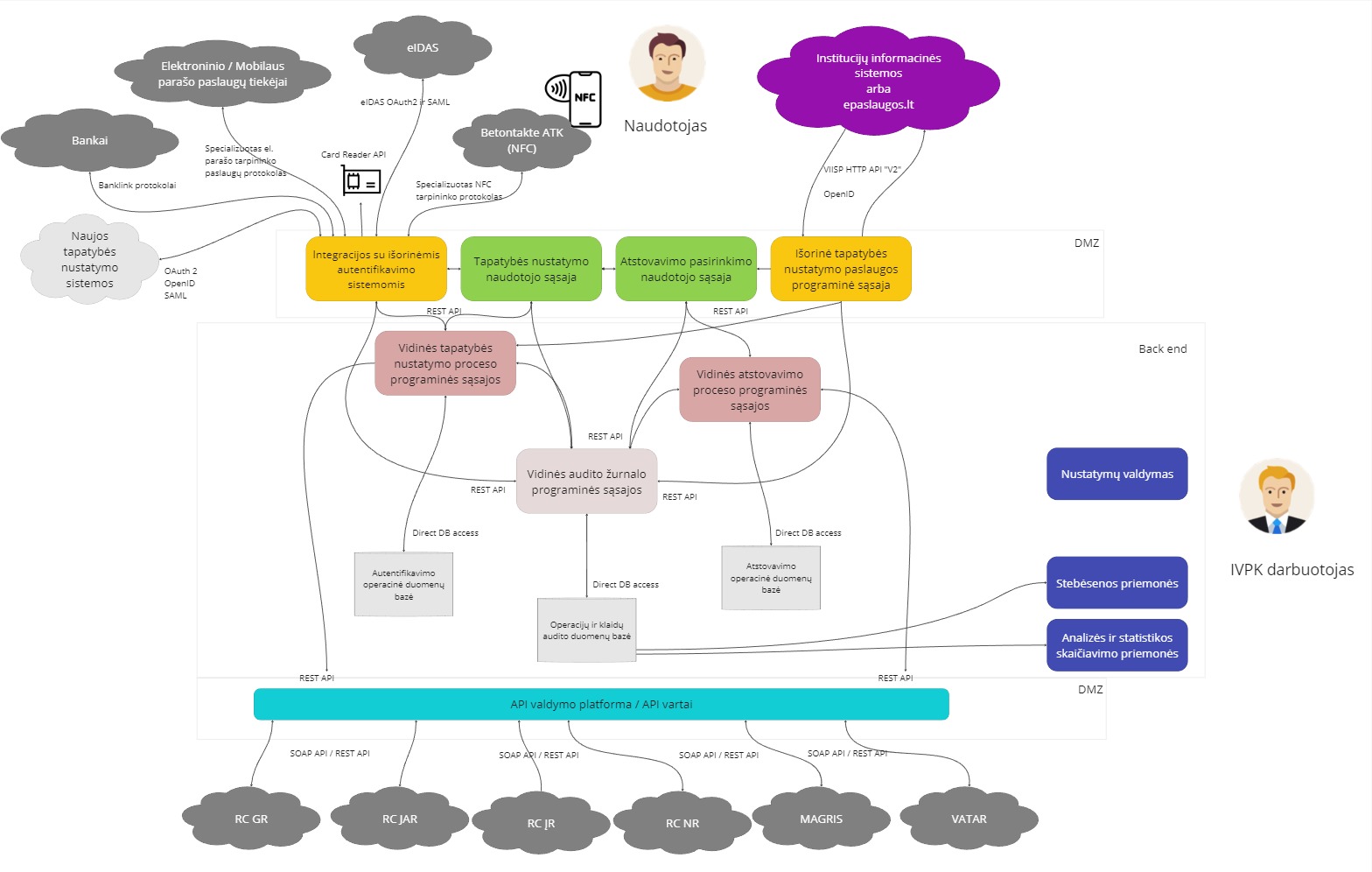
# VI SKYRIUS: REIKALAVIMAI AUTENTIFIKAVIMO POSISTEMEI

## VI.1. Reikalavimai suderinamumui

1. AP turi pilnai atkartoti esamos VIISP autentifikavimo ir atstovavimo nustatymo proceso funkcines savybes (žr. <https://www.epaslaugos.lt/portal/nlogin>, <https://www.epaslaugos.lt/portal/content/1257>) ir realizuoti procesą, aprašytą sk. [V SKYRIUS: AUTENTIFIKAVIMO IR ATSTOVAVIMO NUSTATYMO PROCESAS](#_V_SKYRIUS:_AUTENTIFIKAVIMO).
2. AP turi būti sukurta išlaikant pilną atgalinį suderinamumą (angl. backward compatibility) su visomis be išimties integruotomis informacinėmis sistemomis (tiek tapatybės nustatymo sistemomis, tiek registrais) ir užtikrinti esamos VIISP TNP išorinių integracinių sąsajų, protokolų, formatų ir mechanizmų palaikymą, nereikalaujant išorinių sistemų modifikavimo.
3. Laimėjusiam Tiekėjui bus suteikta prieiga prie VIISP programinio kodo, esamo VIISP autentifikavimo komponento Java programinio kodo (angl. source code) galimam panaudojimui. Priklausomai nuo Tiekėjo siūlomos technologinės platformos, Tiekėjas turės galimybę tiek panaudoti esamo programinio kodo fragmentus tiesiogiai, jeigu bus pasiūlyta realizuoti Java programavimo kalba, tiek kurti alternatyvų programinį kodą pagal esamo Java programinio kodo fragmentų pavyzdžius. Taip pat Tiekėjui bus pateiktos integracijos su išorinėmis tapatybės nustatymo sistemomis specifikacijos, kurios negali būti paviešintos šios Techninės specifikacijos prieduose dėl konfidencialumo apribojimų.
4. PO atsakinga užtikrinti esamo VIISP priežiūros paslaugų tiekėjo palaikymą ir konsultacijas AP sukūrimo, modernizavimo ir diegimo paslaugų Tiekėjui, siekiant technologinio suderinamumo ir funkcinio lygiavertiškumo užtikrinimo.

## VI.2 Reikalavimai programinės įrangos architektūrai

1. Konceptuali AP architektūra, pagrindiniai komponentai, duomenų bazės, sąveika su išorinėmis sistemomis pateikta diagramoje kitame puslapyje:



pav. 3 AP architektūra

| **AP architektūros komponentas \*** | **Aprašymas** | **Sąveika su** |
| --- | --- | --- |
|  | Modulis (-iai), atsakingas už   * abiejų krypčių sąveiką su institucijų informacinėmis sistemomis, kurioms tiekiama autentifikavimo paslauga, * išorinės programinės sąsajos teikimą   + esamo VIISP autentifikavimo protokolo versijos V2 (<https://www.epaslaugos.lt/portal/content/1257>) pagrindu,   + naujo OpenID (<https://openid.net/>) standartu paremto protokolo pagrindu,   + vieningo autentifikavimo (angl. Single Sign On, SSO) tarp skirtingų institucijų informacinių sistemų kontrolės palaikymą minėtų protokolų pagrindu. | Išorinės institucijų IS,  AP komponentai:   * Tapatybės nustatymo naudotojo sąsaja, * Tapatybės nustatymo vidinės programinės sąsajos ir veiklos logika * Audito žurnalo pildymo vidinės programinės sąsajos |
|  | Web pagrindu veikiančios naudotojo sąsajos lygio modulis (-iai) atkartojantys esamą <https://www.epaslaugos.lt/portal/nlogin> sąsajos galimybes ir padengiantis V skyriuje aprašyto proceso autentifikavimo pasirinkimus ir žingsnius (iki atstovavimo pasirinkimo).  Esama naudotojo sąsaja turės būti perdaryta ir suderinta su PO, siekiant pagerinti ergonomiką ir prieinamumą. | AP komponentai:   * Išorinė tapatybės nustatymo paslaugos programinė sąsaja * Integracijos su išorinėmis autentifikavimo sistemomis * Vidinės tapatybės nustatymo proceso programinės sąsajos, * Vidinės audito žurnalo programinės sąsajos |
|  | Modulis (-iai), atsakingas už   * abiejų krypčių sąveiką su išorinėmis tapatybės nustatymo sistemomis ir priemonėmis, * visų esamų integracijų ir protokolų palaikymą   + autentifikavimas per bankus,   + autentifikavimas el. parašu, tiek mobiliuoju , tiek išmaniosios kortelės ar USB laikmenos pagrindu,   + autentifikavimas per eIDAS,   + autentifikavimas bekontaktės išmaniosios kortelės pagrindu NFC protokolo ir mobiliosios programėlės pagrindu. * Naujų protokolų būsimoms integracijoms pavyzdinę realizaciją (angl. reference implementation) – Oauth v2, OpenID, SAML   Plačiau apie integracijas su išorinėmis autentifikavimo sistemomis skyriuje [VI.4 Integracijos su išorinėmis autentifikavimo sistemomis](#_VI.4_Integracijos_su). | Išorinės sistemos:   * Internet bankų sistemos, * El. parašo tarpininkų sistemos, * Bekontakčių NFC kortelių sistemos, * Išmaniųjų kortelių skaitytuvo sistemos, * Kitos būsimos tapatybės nustatymo sistemos   Vidiniai AP komponentai:   * Tapatybės nustatymo naudotojo sąsaja, * Vidinės tapatybės nustatymo proceso programinės sąsajos, * Vidinės audito žurnalo programinės sąsajos |
|  | Modulis (-iai) atsakingi už   * autentifikavimo proceso veiklos logiką (angl. back end), * išorinių institucijų IS perduodamų autentifikavimo paketų apdorojimą, * autentifikavimo paketų, skirtų išorinėms institucijų IS formavimą, * išorinių tapatybės nustatymo sistemų perduotų paketų apdorojimą, * išorinių sistemų nustatytos tapatybės tikrinimą pagal išorinius valstybinius registrus unifikuotų REST API standarto programinių sąsajų, veikiančių per API vartus, pagalba. | Išorinės sistemos:   * tapatybės tikrinimo valstybiniai registrai, * API valdymo platforma / API vartai.   Vidiniai AP komponentai:   * Tapatybės nustatymo naudotojo sąsaja, * Išorinė tapatybės nustatymo paslaugos programinė sąsaja, * Integracijos su išorinėmis autentifikavimo sistemomis, * Autentifikavimo operacinė duomenų bazė, * Vidinės audito žurnalo programinės sąsajos. |
|  | Atskira duomenų bazė, skirta saugoti autentifikavimo proceso nustatymus ir tarpinius autentifikavimo duomenis, pavyzdžiui, vieningo autentifikavimo (SSO) žetonų (ang. token) galiojimą.  Duomenų bazė nekaupia ir nesaugo asmens tapatybės duomenų. | Vidiniai AP komponentai:   * Vidinės tapatybės nustatymo proceso programinės sąsajos |
|  | Web pagrindu veikiančios naudotojo sąsajos lygio modulis (-iai) atkartojantys esamą <https://www.epaslaugos.lt/portal/nlogin> sąsajos galimybes ir padengiantis V skyriuje aprašyto proceso atstovavimo pasirinkimo žingsnius. | Vidiniai AP komponentai:   * Vidinės atstovavimo proceso programinės sąsajos, * Vidinės audito žurnalo programinės sąsajos, * Tapatybės nustatymo naudotojo sąsaja |
|  | Modulis (-iai) atsakingi už   * atstovavimo pasirinkimo proceso veiklos logiką (angl. back end), * autentifikavimo paketų, skirtų išorinėms institucijų IS formavimą, papildant atstovavimo duomenimis, * galimų atstovauti asmenų paiešką išoriniuose valstybiniuose registruose unifikuotų REST API standarto programinių sąsajų, veikiančių per API vartus, pagalba. | Išorinės sistemos:   * Atstovavimo ir įgaliojimų valstybiniai registrai. * API valdymo platforma / API vartai   Vidiniai AP komponentai:   * Atstovavimo pasirinkimo naudotojo sąsaja, * Atstovavimo operacinė duomenų bazė, * Vidinės audito žurnalo programinės sąsajos. |
|  | Atskira duomenų bazė, skirta saugoti atstovavimo proceso nustatymus ir tarpinius pasirinkimus.  Duomenų bazė nekaupia ir nesaugo atstovaujamų asmenų ar įgaliojimų informacijos. | Vidiniai AP komponentai:   * Vidinės atstovavimo proceso programinės sąsajos |
|  | Modulis realizuoja unifikuotas programines sąsajas, kurios turi būti naudojamos iš bet kokio AP komponento operacijų ir klaidų žurnalo kaupimui. | Vidiniai AP komponentai:   * Visi funkciniai komponentai, * Operacijų ir klaidų audito duomenų bazė |
|  | Atskira duomenų bazė, skirta operacijų ir klaidų žurnalui kaupti ir saugoti. Duomenų bazė kaupia tik apdorotus nešifruotus duomenis formatu, tinkamu integracijai į išorines stebėsenos ir statistinės analizės priemones | Išorinės sistemos:   * Stebėsenos priemonės, * Analizės ir statistikos skaičiavimo priemonės   Vidiniai AP komponentai:   * Vidinės audito žurnalo programinės sąsajos, * Stebėsenos priemonės, * Operacijų ir klaidų audito analizės ir statistikos skaičiavimo priemonės |
|  | Standartinės ir/ar specializuotos programinės AP veiklos logikos, diegimo, sąveikumo ir kitų nustatymų valdymo priemonės, aprašyto AP administratoriaus metodinėje medžiagoje.  Automatizuotų priemonių, leidžiančių įkelti nustatymus, tvarkomus kitose sistemose, parengimas. | Vidiniai AP komponentai:   * AP aplinkos ir technologinės sisteminio lygio priemonės, * Autentifikavimo operacinė duomenų bazė, * Atstovavimo operacinė duomenų bazė, * Operacijų ir klaidų audito duomenų bazė |
|  | PO turimos stebėsenos ir žurnalų konsolidavimo priemonės. | AP aplinkos ir technologinės sisteminio lygio priemonės.  Vidiniai AP komponentai:   * Operacijų ir klaidų audito duomenų bazė |
|  | PO turimos duomenų analitikos ir statistikos skaičiavimo priemonės. | Vidiniai AP komponentai:   * Operacijų ir klaidų audito duomenų bazė |
|  | PO turima duomenų mainų programinių sąsajų valdymo ir transformacijų tarp protokolų platforma. | Išorinės sistemos:   * Tapatybės tikrinimo valstybiniai registrai, * Atstovavimo ir paieškos valstybiniai registrai.   Vidiniai AP komponentai:   * Vidinės tapatybės nustatymo proceso programinės sąsajos, * Vidinės atstovavimo proceso programinės sąsajos |

*\* Komponentai turi būti atskiriami programinio kodo, duomenų struktūrų, diegimo paketų lygyje ir realizuojamas tokiu būdu, kad modifikuojant vidinę konkretaus komponento realizaciją kūrimo, palaikymo ar plėtros metu būtų galima kiek įmanoma labiau lokalizuoti programinio kodo pakeitimus, susijusius su išvardintu komponentų specifika, nekeičiant kitų komponentų programinio kodo ar struktūrų. Detali komponentų architektūra, naudojamos technologijos, struktūros ir kt. priklauso nuo Tiekėjo pasiūlymo.*

1. Kuriant AP negali būti naudojama jokia trečios šalies uždaro kodo programinė įranga, išskyrus atviro kodo programinę įrangą ir priemones.
2. Kuriant AP turi būti taikomos šiuolaikiškų technologijų, programavimo kalbų, bibliotekų, gairių (angl. framework) aktualios versijos.
3. AP turi turėti būti realizuota naudojant sluoksninę architektūrą, naudotojo sąsajos (angl. frontend) ir serverinės dalies (angl. backend) komunikacija turi būti realizuota naudojanti REST API programines sąsajas.
4. AP turi būti realizuota kaip būsenos nesauganti (angl. stateless) aplikacija; AP naudotojas turi būti nepririšamas prie konkretaus aplikacijos serverio, kiekvieną naudotojo užklausą turi galėti apdoroti bet kuris aplikacijos serveris. Naudotojui baigus darbą sistemos resursai turi būti atlaisvinami iš kart - sistemoje naudotojo sesija neturi būti saugoma, išskyrus vieningo autentifikavimo (angl. Single Sign On, SSO) žetonų (angl. token) ir jų galiojimo informacijos saugojimą, būtiną SSO veikimui.
5. AP turi būti sukurta taip, kad bet kurio architektūrinio sluoksnio programinė įranga galėtų būti diegiama keliuose serveriuose ir tarp jų organizuojamas apkrovos pasiskirstymas (t.y. neturi būti ribojamas aktyvių elementų / veikiančių mazgų skaičius).
6. Duomenų saugyklų lygyje turi būti taikomos reliacinių duomenų bazių valdymo sistemos.
7. AP turi būti pilnai atskirta ir atskirai diegiama bei administruojama nuo esamos VIISP.
8. AP duomenų bazės turi būti pilnai atskirtos ir atskirai diegiamos bei administruojamos nuo VIISP duomenų bazės (-ių).
9. AP duomenų bazės turi būti atskirtos pagal paskirtį, paliekant galimybę atskirai diegti ir administruoti. Tai leis kritinio gedimo atveju greitai atstatyti AP, panaudojant rezervines duomenų kopijas, naujoje produkcinėje aplinkoje, o taip pat įgalins taikyti mikroservisų architektūrą tiek viduje AP, o galimai ir būsimoms išorinėms AP programinėms sąsajoms:
   1. Autentifikavimo operacinė duomenų bazė, kurioje turi būti saugomi tik tie nustatymai ir duomenys, kurie yra būtini sąveikos su išorinėmis sistemomis, tapatybės nustatymo, tapatybės patikros procesui atlikti,
   2. Atstovavimo operacinė duomenų bazė, kurioje turi būti saugomi tik tie nustatymai ir duomenys, kurie yra būtini atstovavimo pasirinkimui ir sąveikos su išorinėmis sistemomis procesui atlikti,
   3. Operacijų ir klaidų audito žurnalo duomenų bazė, kurioje visi AP moduliai registruos veiklos įvykius ir klaidas. Ši duomenų bazė turi būti realizuota DBVS platformoje, kuri palaiko duomenų dalijimosi (angl. partitioning) mechanizmus, užtikrinant galimybę skirstyti duomenis pagal istorinius periodus ir atskirai archyvuoti senus duomenis.
10. AP turi būti projektuojama taip, kad kritinio gedimo atveju atstačius tik Autentifikavimo operacinę duomenų bazę ir Atstovavimo operacinę duomenų bazę turi veikti AP funkcionalumas be operacijų ir klaidų audito.
11. AP išorinės programinės sąsajos, skirtos sąveikai su institucijų informacinėmis sistemomis, kuriomis teikiama autentifikavimo paslauga, turi būti realizuotos panaudojant esamos VIISP TNP standartus ir protokolus (žr. [VI.1. Reikalavimai suderinamumui](#_VI.1._Reikalavimai_suderinamumui)), o konkrečiai – esamą VIISP HTTP API sąsają (versija V2), aprašyta <https://www.epaslaugos.lt/portal/content/1257>, ir nauja OpenID standartu paremta sąsaja. V2 protokolo realizacija turi apimti vieningo autentifikavimo (SSO) kontrolės sąsajas, skirtas automatiniam tapatybės duomenų perdavimui ir sesijos atstatymui, persijungiant tarp skirtingų institucijų informacinių sistemų.
12. AP išorinės programinės sąsajos, skirtos sąveikai su išorinėmis tapatybės nustatymo sistemomis turi būti realizuotos panaudojant esamos VIISP TNP standartus ir protokolus (žr. [VI.1. Reikalavimai suderinamumui](#_VI.1._Reikalavimai_suderinamumui)). Papildomai turi būti realizuotas modernių autentifikavimo protokolų, tokių, kaip OAuth v2, SAML, OpenID palaikymas būsimoms integracijoms su išorinėmis tapatybės nustatymo sistemomis. AP, kaip tapatybės duomenų gavėjas, turi turėti galimybę duomenis gauti Oauth v2. SAML, OpenID arba specialiais, tapatybės duomenų teikėjo aprašytais formatais;
13. Vidinės API programinės sąsajos turi būti realizuotos vadovaujantis OpenAPI v.3.0, JSON/REST API standarto pagrindu.
14. AP sąveika su tapatybės patikros registrais ir atstovavimo nustatymo registrais, kur tai leidžia techninės galimybės, turi būti realizuota vadovaujantis OpenAPI v.3.0, JSON/REST API standartu, panaudojant tarpinę PO turimą API valdymo / API vartų (angl. API Gateway) Gravitee API Gateway (https://www.gravitee.io/platform/api-gateway) programinės įrangos platformą (toliau – API GW). API GW veiks, kaip unifikuotas vidinis REST API sluoksnis, realizuojantis reikiamas transformacijas į išorinių valstybinių registrų SOAP API ar REST API sąsajas API GW terpėje ir priemonėmis (įskaitant galimą šifravimą ar pasirašymą VIISP AP vardu).
    1. Sukurti naują API ir jį sukonfigūruoti API GW platformoje bendradarbiaujant kartu su PO ekspertais. PO užtikrins būtina API GW ekspertų dalyvavimą ir palaikymą. Naujam API turės būti sukofigūruota integracinių sąsajų transformacija iš vidinių AP REST API formatų į išorinių registrų palaikomus užklausų formatus (SOAP API, REST API ar kitas). Užklausų ir atsakymų transformaciją atliks API GW.
    2. PO atsakinga užtikrinti Tiekėjo prieigą prie API GW platformos, apmokymą bei gamintojo palaikymą būtiniems darbams atlikti.
15. AP architektūra ir reikalavimai produkcinės diegimo aplinkos resursams turi užtikrinti ne lėtesnį nei 100ms uždelsimo (angl. Latency) integracinių sąsajų atsaką, esant 500 transakcijų per sekundę apkrovimui, nevertinant nuo AP nepriklausomų veiksnių (tinklo greitaveikos, kitų sistemų, įskaitant API GW ir išorinių valstybinių registrų, greitaveikos).
16. AP architektūra ir reikalavimai produkcinės diegimo aplinkos resursams turi užtikrinti ne lėtesnį nei 3 sek. naudotojo sąsajos atsaką, vienu metu dirbant 10 000 išorinių naudotojų (matuojant atsaką naudotojo sąsajos lygyje ir nevertinant viešo tinklo greitaveikos). Galimi išimtiniai atvejai, kurie turi būti suderinti su PO (pvz. ataskaitų generavimas, duomenų importavimas ar eksportavimas, didelės apimties rinkmenų įkėlimas, veiksmai apimantys užklausas ir atsakymų gavimus iš trečių šalių sistemų ir kt.).
17. Architektūra turi palaikyti AP nefunkcinių pajėgumų plėtros galimybes prijungiant papildomą techninę įrangą arba virtualią infrastruktūrą;
18. Turi būti sudarytos AP plėtros galimybės neatliekant papildomų sistemos perprojektavimo ar realizavimo darbų papildyti sistemą naujais skaičiavimo ar saugyklų resursais. Pajėgumų didinimas turi būti atliekamas nestabdant sistemos darbo.
19. AP architektūra neturi būti ribojantis veiksnys ateityje plėsti ir/ar modifikuoti specializuotos programinės įrangos funkcionalumą. Architektūra turi būti projektuojama daugiapakopės architektūros pagrindu taip, sudarant jos funkcinės plėtros atskirų sluoksnių lygmenyse galimybes.

## VI.3 Reikalavimai naudotojo sąsajai

1. AP naudotojo sąsaja įgyvendinama taikant šiuolaikiškas žiniatinklio (angl. Web site) priemones.
2. Įgyvendinant AP naudotojo sąsają, kiek įmanoma, turi būti pasitelkta grafinio dizaino rezultatais, pateikiamais šio dokumento priede (Priedas Nr. 2 – Naujas Web dizainas.zip).
3. AP naudotojo sąsaja turi būti suderinama su populiariomis rinkoje interneto naršyklėmis ir jų aktualiomis versijomis (detalios naršyklių versijos turi būti suderintos įgyvendinimo eigoje): Microsoft Edge, Mozilla Firefox, Safari, Google Chrome.
4. AP naudotojo sąsaja turi būti realizuota lietuvių ar anglų kalbomis. Kalba turi būti naudojama laikantis bendrinių kalbos taisyklių. Data, laikas ir kiti parametrai turi būti naudojami tokiu formatu, koks yra naudojamas Lietuvoje.
5. AP naudotojo sąsajos architektūra turi numatyti galimybę praplėsti kalbų sąrašą ateityje.
6. AP naudotojo sąsaja turi būti suderinama su interneto naršyklių automatinio kalbos vertimo įrankiais, kurie įgalins kelias dešimtis papildomų kalbų.
7. AP naudotojo sąsaja turi būti pritaikyta reikalavimams, kurie keliami neįgaliesiems pritaikytų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainių kūrimo, testavimo ir įvertinimo metodinėse rekomendacijose, patvirtintose Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Susisiekimo ministerijos direktoriaus 2013 m. gegužės 23 d. įsakymo Nr. T-72 Dėl Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004 m. kovo 31 d. įsakymo Nr. T-40 ‚Dėl Neįgaliesiems pritaikytų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainių kūrimo, testavimo ir įvertinimo metodinių rekomendacijų patvirtinimo‘ pakeitimo“. Remiantis įsakymo 7 punktu „Rekomenduojama siekti interneto svetainę pritaikyti ne žemesniu kaip AA lygiu“, Tiekėjas turi užtikrinti „AA“ lygmens pasiekiamumą pagal „Web Content Accessibility Guidelines 2.1“ skaitmeninio turinio prieinamumo gaires (https://www.w3.org/TR/WCAG21/).
8. AP naudotojo sąsaja turi įgyvendinti interneto turinio prieinamumo užtikrinimo gaires (WCAG), turinys turi būti pateikiamas tokia forma, kad klausos ir regos negalią turintys asmenys galėtų naudotis AP funkcionalumu.

## VI.4 Integracijos su išorinėmis autentifikavimo sistemomis

1. Tapatybės nustatymo procesui realizuoti AP remiasi trečių šalių teikiamomis paslaugomis (angl. web-services). PO turi sudariusi atskiras sutartis su paslaugų teikėjais tokios paslaugoms gauti. Tiekėjui bus pateikta dokumentacija atitinkamoms integracijoms realizuoti. Šiuo metu išoriniai paslaugos teikėjai teikia šias paslaugas:
   1. Tapatybės nustatymo paslaugos teikėjas:
      1. Sertifikato, saugomo fizinėje laikmenoje, informacijos gavimas, parašo sudarymas naudojant specializuotą PĮ, diegiamą naudotojo naršyklėje (angl. Browser plug-in);
      2. Parinkčių, rodomų naršyklės įskiepyje, konfigūravimo API;
      3. Sertifikato informacijos patikrinimas (sertifikato galiojimo, atšaukimo informacija);
      4. Sertifikato informacijos gavimas ir parašo tikrinimas, kai naudojama mobili atpažinties priemonė;
   2. eIDAS nacionalinis mazgas:
      1. Užsienio piliečio atpažinties duomenų gavimo inicijavimas ir duomenų gavimas;
      2. Lietuvos piliečio, siekiančio gauti paslaugą užsienio valstybėje, duomenų perdavimas iš AP į nacionalinį mazgą;
   3. Asmens tapatybės kortelės duomenų, gaunamų naudojant NFC protokolą, gavimas naudojant mobiliąją programėlę mCARD:
      1. PKI operacijų, atliekamų luste, vykdymas naudojant NFC technologiją, per pateiktą integracinę sąsają;
   4. Lietuvoje veikiančios bankų, kredito unijų ir kitų institucijų, teikiančių asmens tapatybės nustatymo paslaugą, sistemos:
      1. Asmens tapatybės duomenų gavimas, kai paslauga inicijuojama tiek iš AP, tiek tiesiogiai iš institucijos sistemos. Šiuo metu yra realizuota 10 integracijų su tokio tipo institucijomis, kurios turės būti realizuotos AP.

## VI.5. Reikalavimai autentifikavimo ir saugos standartų palaikymui

1. Kaip jau buvo nurodyta skyriuje [VI.1. Reikalavimai suderinamumui](#_VI.1._Reikalavimai_suderinamumui), AP turi palaikyti visus šiuo metu veikiančius VIISP integruotos autentifikavimo paslaugos saugos mechanizmus, įskaitant SSO sprendimą.
2. Autentifikavimo mechanizmo architektūra ir realizacija turi įgalinti ir teikti atitinkamas integracines sąsajas trečiųjų šalių autentifikavimui naudojant esamus (VIISP HTTP API V2) ir naują (OpenID) protokolus.
3. Vidinių ir išorinių integracinių sąsajų (angl API, endpoints) šifravimas perduodant duomenis TLS/SSL protokolais.
4. Jautrių duomenų šifravimas AP duomenų bazėse naudojant AES ar panašius algoritmus, užtikrinant saugias šifravimo raktų valdymo praktikas.
5. Turi būti naudojamos ir diegiamos šiuolaikinės priemonės, apsaugančios perduodamus duomenis ir integralumą tiek transporto, tiek aplikacijos, tiek duomenų saugyklos lygyje.
6. Pasirinkta architektūra ir technologijos turi užtikrinti OWASP TOP10 įvardintų rizikų prevenciją:
   1. Duomenų ir duomenų perdavimo kanalo šifravimas,
   2. Saugių ir atnaujintų kriptografinių protokolų naudojimas API sąveikoms.
   3. Saugių slapukų (cookies) naudojimas, kurie yra HTTPOnly ir pažymėti kaip 'Secure'.
   4. SameSite atributų taikymas slapukams, siekiant užkirsti kelią CSRF atakoms.
   5. Įvesties validavimas ir sanitizacija: Griežtas įvesties validavimas, siekiant išvengti SQL injekcijos, XSS ir kitų įsiskverbimo atakų.
   6. Saugos antraštės ir CSP: HTTP saugos antraščių, pavyzdžiui, Turinio Saugumo Politikos (CSP), X-Frame-Options, X-Content-Type-Options ir Referrer-Policy įgyvendinimas.
   7. Apsauga nuo sesijos fiksacijos ir pagrobimo.
   8. Ribojimas ir slopinimas (angl. Rate Limiting and Throttling):
   9. Ribojimas API ir prisijungimo bandymų, siekiant išvengti „grubios jėgos“ (angl. brute force) atakų. Slopinimo mechanizmai apkrovai valdyti ir apsaugoti nuo DoS atakų.
   10. Audito įrašai ir žurnalizavimas, žr. [VI.5. Reikalavimai audito žurnalų valdymui](#_VI.5._Reikalavimai_audito).

## VI.6. Reikalavimai audito žurnalams ir jų valdymui

1. AP turi rinkti, kaupti, saugoti dedikuotoje duomenų bazėje visas AP operacijas ir/ar sutrikimus, įskaitant, bet neapsiribojant:
   1. Naudotojų apsilankymai AP puslapyje,
   2. Institucijų IS nukreipimai į AP tolesniam autentifikavimui,
   3. Autentifikavimo būdo pasirinkimus,
   4. Nukreipimus į išorinę tapatybės nustatymo sistemą pagal pasirinktą autentifikavimo būdą,
   5. Tapatybės nustatymo išorinėje tapatybės nustatymo sistemoje rezultatus (be asmens duomenų – tik sėkmė/nesėkmė),
   6. Kito asmens atstovavimo pasirinkimo faktus,
   7. Sėkmingo tapatybės nustatymo faktus,
   8. Sėkmingo atstovavimo pasirinkimo faktus,
   9. Tapatybės duomenų perdavimo išorinėms institucijų IS,
   10. Kreipiniai ir atsakymai iš asmens tikrinimo ir/ar atstovaujamų asmenų patikros registrų (be asmens duomenų – tik sėkmė/nesėkmė)
   11. Bet kokie išorinių sistemų kreipiniai per integracines sąsajas. Veiksmai, atlikti per AP API, turi būti audituojami analogiškai veiksmams, atliekamiems per naudotojo sąsają
2. Klaidos, sutrikimai, incidentai, tiek sisteminiai, tiek AP programinės įrangos, tiek išorinių sistemų perduotos klaidos ir techniniai pranešimaineprivalo būti kaupiami dedikuotoje audito duomenų bazėje, tačiau turi būti kaupiamos žurnaluose tokiu būdu, kad užtikrinti galimybę automatiškai įkelti tuos žurnalus į standartinę žurnalų konsolidiavimo, paieškos ir analizės platformą GrayLog ar lygiavertę..
3. Audito žurnalo realizacija ir duomenų struktūra turi užtikrinti galimybę taikyti standartines duomenų analitikos ir statistikos skaičiavimo Microsoft Power BI ar lygiavertes priemones, taip pat taikyti standartines žurnalų konsolidavimo, paieškos ir analizės platformą GrayLog ar lygiavertes priemones. Duomenų struktūros turi leisti koreliuoti įvykius žurnale tiek tuomet, kai naudotojas dar nėra autentifikuotas, tiek po to. Tiekėjas nėra atsakingas už pačių analitikos, statistikos ir paieškos priemonių tiekimą ir realizaciją, tačiau turi pateikti reikiamą metodinę medžiagą. .
4. Duomenys, saugomi audito DB, turi būti struktūrizuoti. Pradinių (nestruktūrizuotų) duomenų saugojimo pore[ikis bus nustatomas analizės ir projektavimo etapo metu.
5. AP sudaranti programinė įranga, rašanti papildomą techninę informaciją į techninius žurnalus (angl. Application log) turi laikytis bendrų principų, leidžiančių šia informaciją koreliuoti naudojant žurnalų agregavimo įrankius (pvz. GrayLog).

## VI.7. Reikalavimai stebėsenos galimybėms

1. Specializuota programinė įranga turi būti kuriama tokiu būdu ir naudojant tokias technologijas, kad PO galėtų atlikti pilnavertę gamybinės aplinkos ir programinės įrangos veikimo stebėseną (angl. monitoring) PO šiuo metu naudojamos Zabbix (tinklo ir sisteminio lygio platformų stebėsena) ir IBM QRadar SIEM (saugos įvykių stebėsena) programinės įrangos pagalba.
2. Operacijų ir klaidų audito žurnalų realizacija turi užtikrinti galimybė integruoti tiek loginių operacijų, tiek sisteminių klaidų ir pranešimų įvykius į šiuo metu PO naudojamą GrayLog platformą (žurnalų konsolidavimas ir analizė) ar lygiavertę.
3. Taikant išvardintas priemones (GrayLog ar lygiavertę) turi būti užtikrinta galimybę identifikuoti:
   1. AP diegimo aplinkos ir atskirų jos mazgų neprieinamumą,
   2. AP diegimo aplinkos ir atskirų jos elementų resursų trūkumą, ribines ar anomalines apkrovas,
   3. AP visumos ar atskirų AP komponentų ar duomenų bazių neprieinamumą,
   4. AP sisteminės programinės įrangos, AP specializuotos programinės įrangos, AP duomenų bazių, vidinių ir išorinių integracinių sąsajų klaidas,
   5. AP komponentų našumo kritimus.
4. Projekto eigoje Tiekėjas turi atlikti detalią PO stebėsenos poreikių ir galimybių analizę ir realizuoti ir/arba aprašyti metodinėje medžiagos AP stebėsenos priemones.

## VI.8. Reikalavimai integracijoms

1. Kaip pavaizduota architektūros diagramoje sk. [VI.2 Reikalavimai programinės įrangos architektūrai](#_VI.2_Reikalavimai_programinės) AP turi būti integruota su:
   1. Išorinėmis institucijų sistemomis, kurioms reikalinga naudotojo tapatybės nustatymo paslauga:
      1. Bet kokia institucijos, sudariusios tapatybės nustatymo paslaugos sutartį su VSSA, informacinė sistema,
      2. VIISP.
   2. Tapatybės nustatymo sistemomis. Žr. [V SKYRIUS: AUTENTIFIKAVIMO IR ATSTOVAVIMO NUSTATYMO PROCESAS](#_V_SKYRIUS:_AUTENTIFIKAVIMO) , reikalavimai 12.3.
   3. Tapatybės patikros registrais. Žr. [V SKYRIUS: AUTENTIFIKAVIMO IR ATSTOVAVIMO NUSTATYMO PROCESAS](#_V_SKYRIUS:_AUTENTIFIKAVIMO) reikalavimai 13.1.
   4. Atstovavimo registrais. Žr. Žr. [V SKYRIUS: AUTENTIFIKAVIMO IR ATSTOVAVIMO NUSTATYMO PROCESAS](#_V_SKYRIUS:_AUTENTIFIKAVIMO) reikalavimai 13.2.
   5. PO API valdymo / API vartų sistema Gravitee API Gateway (https://www.gravitee.io/platform/api-gateway)
   6. PO stebėsenos sistemos Zabbix ir IBM QRadar SIEM.
   7. PO audito žurnalų analizės sistema GrayLog.

## VI.9 Reikalavimai duomenų ir konfigūracijos migravimui

1. Į AP turi būti perkelti visų esamų VIISP TNP naudotojų - Institucijų IS nustatymai.
2. Į AP turi būti perkelti visų tapatybės nustatymo sistemų nustatymai.
3. Preliminarus VIISP TNP nustatymų elementų sąrašas, kuris turės būti peržiūrėtas ir iškeltas iš VIISP į AP, pateikiamas Priede 2 AP nustatymų sąrašas, tiek migruojamas iš VIISP, tiek naujai papildomas, turi būti peržiūrėtas, suprojektuotas, dokumentuotas ir suderintas su PO projekto įgyvendinimo eigoje..
4. AP turi būti pasiekiama esamoms Institucijų IS be jokių programinio kodo pakeitimų.
5. Tapatybės nustatymo sistemos turi pripažinti ir sąveikauti su AP be jokių programinio kodo pakeitimų.

## VI.10 Reikalavimai VIISP modifikavimui

1. AP sukūrimo, modernizavimo ir diegimo Sutartis neapima VIISP modifikavimo paslaugų. Tačiau suprantama, kad perspektyvoje VIISP TNP turi būti demontuota arba kitaip deaktyvuota VIISP sistemoje ir VIISP el. paslaugos turi tapti viena iš Institucijų IS AP atžvilgiu.
2. Tam tikslui, AP Tiekėjas turi užtikrinti bendradarbiavimą, informacijos mainus, specifikacijų ir sąsajų derinimą su VIISP priežiūros paslaugų tiekėju, siekiant parengti VIISP TNP demontavimo/deaktyvavimo specifikaciją ir planą.

## VI.11 Reikalavimai diegimui

1. AP turi būti diegiama Valstybės informacinių technologijų centro (toliau - VITC) valdomoje valstybinio duomenų centro debesijos infrastruktūroje ir atitikti VITC paslaugų katalogo <https://servicedesk.vitc.lt/docs/pages/viewpage.action?pageId=3768653> platformas ir paslaugas.
2. AP turi būti diegiama naudojant konteinerizacijos mechanizmus.
3. AP architektūra, naudojamos programinės įrangos ir konteinerizacijos priemonės turi leisti diegimą ir/ar atstatymą į vieną ar daugiau globalios viešosios debesijos platformų - Microsoft Azure, Amazon Web Services, Google Cloud ar lygiavertę, tačiau neturi turėti technologinio prisirišimo prie išvardintų debesijos platformų specializuotų paslaugų.
4. AP turi būti diegiama VITC debesijos infrastruktūroje į aplinkas, aprašytas lentelėje žemiau:

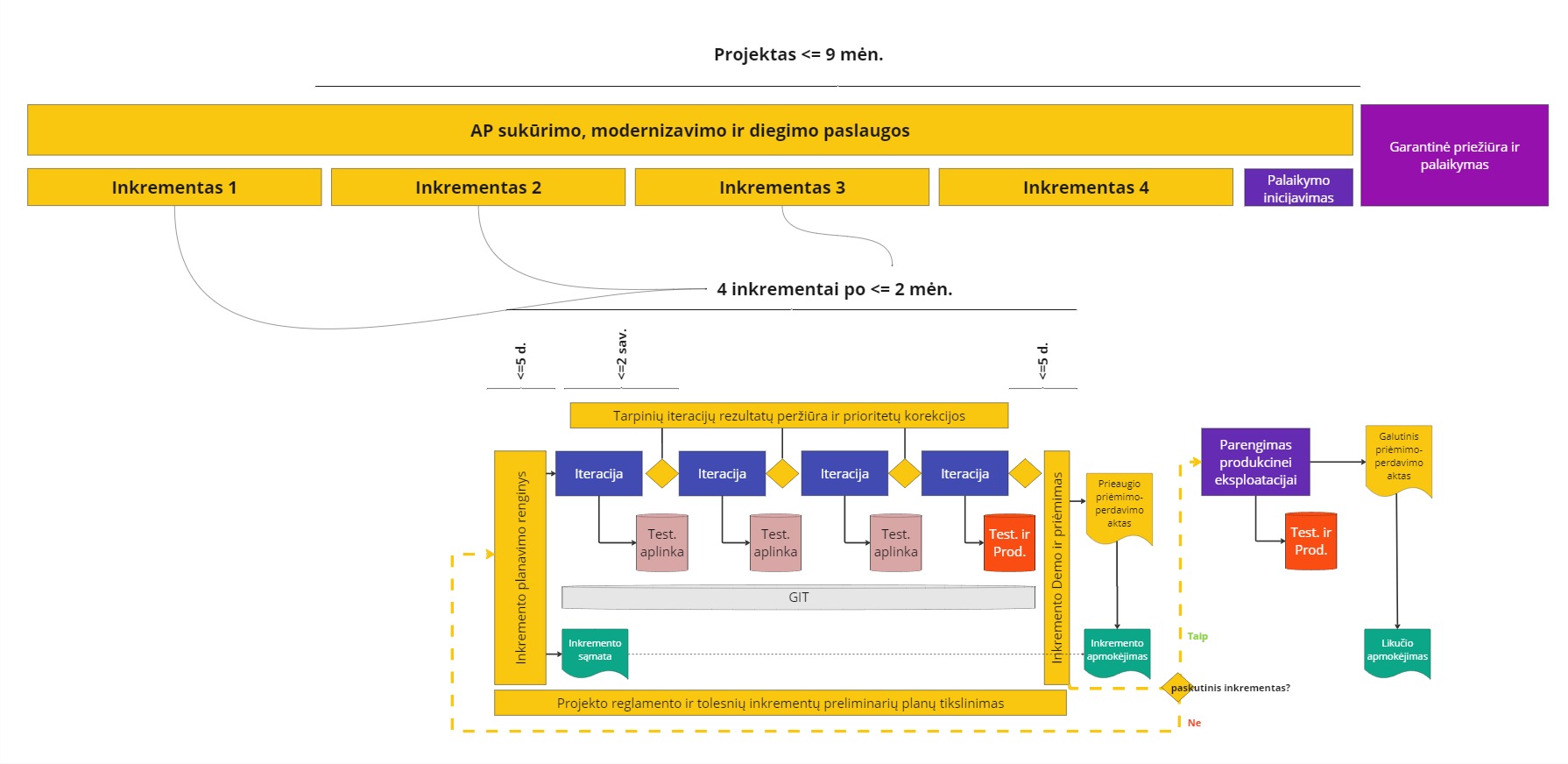
| **Aplinka** | **Paskirtis** | **Naudotojai** | **Aukšto prieinamumo poreikis** |
| --- | --- | --- | --- |
| Programavimo | Neintegruotas AP funkcionalumo pakeitimų testavimas programavimo eigoje. | Tiekėjas,  VSSA projekto komanda. | Ne |
| Testavimo | Integruotas naujų AP versijų pakeitimų testavimas. | Tiekėjas,  VSSA projekto komanda,  VSSA partneriai/atstovai, atsakingi už kitų institucijų informacinių sistemų integraciją su AP. | Ne |
| Priėmimo testavimo | Integruotas naujų AP versijų priėmimo testavimas . | VSSA projekto komanda,  VSSA partneriai/atstovai, atsakingi už kitų institucijų informacinių sistemų integraciją su AP. | Taip |
| Produkcinė | AP funkcinis naudojimas pagal paskirtį ir kitos operacijos. | Išorės naudotojai,  VSSA darbuotojai – AP priežiūros ir administravimo tarnyba,  VITC administratoriai. | Taip |

1. Tiekėjas turi aprašyti **savo pasiūlyme** ir tikslinti projekto eigoje išvardintų AP diegimo aplinkų diegimo architektūrą, įskaitant
   1. sistemines programinės įrangos priemones,
   2. infrastruktūros resursų reikalavimus kiekvienai aplinkai,
   3. krūvio balansavimo ir maršrutizavimo priemones,
   4. aukšto prieinamumo užtikrinimo priemones,
   5. integracijos su ugniasiene (WAF) reikalavimus,
   6. SSL/TLS sertifikatai iš patikimų Sertifikatų Išdavimo Institucijų.
2. AP ir tolesnių versijų diegimai turi būti vykdomi minimizuojant galimas prastovas iki 1 val.
3. AP versijų diegimas į Testavimo ir Produkcinę aplinkas projekto eigoje turi būti automatizuotas, panaudojant VITC versijų valdymo ir diegimo automatizavimo priemones, integruotas į VITC valstybės duomenų centro aplinkas. Detali VITC diegimo procesų ir įrankių informacija bus pateikta Tiekėjui, pasirašius Sutartį.

# VII SKYRIUS: REIKALAVIMAI PASLAUGŲ TEIKIMUI

## VII.1 Reikalavimai įgyvendinimo būdui ir paslaugų teikimo etapams

1. AP sukūrimo, modernizavimo ir diegimo paslaugos turi būti suteiktos ne vėliau nei per 9 (devynis) mėnesius nuo Sutarties pasirašymo.
2. Diagrama kitame puslapyje (pav. 4) ir reikalavimai žemiau aprašo principinį įgyvendinimo būdo modelį:
3. AP turi būti įgyvendinama iteraciniu-inkrementiniu būdu (angl. Agile) taikant ne ilgesnes nei 2 (dviejų) savaičių trukmės iteracijas, kurių gale Tiekėjas demonstruoja veikiančią programinę įrangą Programavimo aplinkoje; ir ne retesnius nei 2 (dviejų) mėnesių trukmės etapus - inkrementus, kuomet PO testuoja veikiančią programinę įrangą Testavimo aplinkoje ir/arba vykdo bandomąją eksploataciją Produkcinėje aplinkoje, suderinus su PO.
4. Ne vėliau nei po 10 (dešimties) darbo dienų po Sutarties pasirašymo turi būti sudarytas Projekto reglamentas, kuris turi būti reguliariai atnaujinamas Šaliu susitarimu projekto eigoje ir turi apimti:
   1. Projektinę organizaciją - atsakingus asmenis, komandas, projekto valdymo komitetą,
   2. Įrankius, aplinkas, komunikacijos valdymo priemones,
   3. Įgyvendinimo būdo, inkrementų ir iteracijų valdymo darbinius susitarimus,
   4. Inkrementų planavimo renginių tvarką ir tvarkaraštį,
   5. Visų inkrementų preliminarius planus, apimant, bet neapsiribojant:
      1. Inkrementų tikslus,
      2. Preliminarias funkcinę, technologinę ir dokumentų artefaktų apimtį, susiejant su Techninės specifikacijos reikalavimais,
      3. Preliminarias finansines sąmatas,
      4. Kalendorinius terminus,
      5. Diegimo aplinkas.
   6. Patikslintą ir fiksuotą einamojo inkremento planą,
   7. Pasibaigusių inkrementų rezultatų vertinimą,
   8. Projekto pakeitimų valdymo žurnalą,
   9. Projekto rizikų žurnalą.



pav. 4 Įgyvendinimo būdo modelis

1. Patikslintas einamojo inkremento planas sudaromas per pirmas 5 (penkias) darbo dienas nuo inkremento kadencijos pradžios aktyviai bendradarbiaujant Tiekėjui ir PO inkremento planavimo renginio (angl. Program Increment Planning Event) metu, kuris turi būti organizuojamas vadovaujantis SAFe metodikos principais <https://scaledagileframework.com/pi-planning/> ir Projekto reglamente aprašyta ir suderinta tvarka. Einamojo inkremento planas tvirtinamas PO ir turi apimti:
   1. Inkremento tikslus,
   2. Funkcinę, technologinę ir dokumentų apimtį, susiejant su Techninės specifikacijos reikalavimais,
   3. Inkremento finansinę sąmatą, apimant reikalavimo Nr. 103 lentelėje išvardintą pirkimo objekto dalies „AP sukūrimo, modernizavimo ir diegimo paslaugos“ bendros kainos procentą bei suderintų su PO ekspertinių paslaugų valandų kiekį ir jų bendrą kainą bei patikslintą kalendorinį planą,
   4. Priėmimo kriterijus, inkremento užbaigtumo apibrėžimą (angl. Definition of Done, DoD).
   5. Priėmimo procedūras,
   6. Diegimo aplinkas.
2. Kiekvieno inkremento rezultatai turi atitikti inkremento užbaigimo apibrėžimą (DoD), kuris turi būti tikslinamas ir suderinamas Tiekėjo ir PO inkremento planavimo renginio metu (žr. žemiau) ir privalės apimti:
   1. Ankstesnių inkrementų veikiantį ir/ar pagerintą funkcionalumą,
   2. Naujo inkremento suderintos apimties veikiantį funkcionalumą,
   3. Išeities kodą PO GIT (Tiekėjas turi užtikrinti išeities kodo, projektinių užduočių ir darbų eilės (angl. backlog), tarpinių ir galutinių specifikacijų versijų bei kitų darbų eigos skaidrumą PO, naudojant PO suteiktas išeities kodo, versijų ir darbų valdymo platformos (toliau – PO GIT) priemones Microsoft GitHub (https://github.com/) programinės įrangos pagrindu,
   4. Versijų surinkimo, diegimo ir testavimo automatizacijos procesus PO GIT,
   5. Programinės įrangos komponentų funkcionalumo ir/ar architektūros specifikacijas PO GIT,
   6. Patikslintus arba patvirtintus ankstesnius reikalavimus diegimo aplinkų infrastruktūrai.
3. Kiekvieno inkremento paskutinės iteracijos gale turi įvykti inkremento priėmimo renginys, skirtas PO atstovams, nurodytiems Projekto reglamente. Renginio metu vykdoma:
   1. rezultatų demonstravimą,
   2. apsikeitimą grįžtamuoju ryšiu,
   3. pastabų ir trūkumų žurnalo pildymą,
   4. tolesnių darbų prioritetų, apimties ir reikalavimų tikslinimą bei kitokį pasirengimą tolesnio inkremento planavimui,
   5. sprendimą dėl einamojo inkremento priėmimo-perdavimo akto pasirašymo ar esminių trūkumų akto sudarymo,
   6. kitas Projekto reglamente suderintas veiklas.
4. **Pirmo inkremento** rezultate (po pirmų 2 mėn. nuo Sutarties pasirašymo) Tiekėjas turi pristatyti **tarpinę AP versiją**, tinkamą bandomajai eksploatacijai, kuri įgyvendina proceso, aprašyto skyriuje [V SKYRIUS: AUTENTIFIKAVIMO IR ATSTOVAVIMO NUSTATYMO PROCESAS](#_V_SKYRIUS:_AUTENTIFIKAVIMO), dalį su apribojimais ir išlygomis:
   1. Realizuota autentifikavimo naudotojo sąsaja, lygiavertę esamai VIISP TNP naudotojo sąsajai <https://www.epaslaugos.lt/portal/nlogin> ir priderintą prie dizaino reikalavimų (žr. [VI.3 Reikalavimai naudotojo sąsajai](#_VI.3_Reikalavimai_naudotojo)),
   2. Realizuotos autentifikavimo išorinės paslaugos, įskantant sąsajas, protokolų, formatų ir mechanizmų palaikymą:
      1. Institucijos IS autentifikavimo paslaugos užklausos priėmimas ir apdorojimas pagal VIISP TNP specifikaciją (<https://www.epaslaugos.lt/portal/content/1257>),
      2. Su PO suderintos Banklink integracijos su tapatybės nustatymo paslaugą teikiančiais bankais (pvz. <https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PRODE24296774>) palaikymas tiek siunčiant iškvietimą bankui, tiek priimant banko tapatybės nustatymo sistemos rezultatus.
   3. AP autentifikavimo operacinė duomenų bazė su visais nustatymais ir duomenimis, būtinais tapatybės nustatymui per Banklink,
   4. AP versija įdiegta PO arba Tiekėjo testavimo aplinkoje (konkreti aplinka bus suderinta šalių susitarimu inkremento plano tikslinimo metu),
   5. AP versija testuojama su bandomosios Institucijos IS stimuliatoriumi, kurį turi realizuoti Tiekėjas,
   6. AP versija testuojama su PO suderinto banko Banklink testavimo aplinka.
   7. AP programinis kodas išsaugotas PO GIT be pilno versijų valdymo, diegimo ir testavimo automatizavimo.
5. Jeigu pirmojo inkremento tikslas nepasiektas per nustatytą terminą arba turi esminių trūkumų, PO turi teisę neatlygintinai nutraukti paslaugų Sutartį ir pritaikyti Tiekėjui baudas ir/arba sankcijas už padarytą žalą SPP Projekto eigai ir sukeltą riziką. Esminiais trūkumais laikoma, kai nepasiektas pirmojo inkremento rezultatas per 2 mėnesius nuo sutarties įsigaliojimo pradžios ir neįgyvendinta bent vienas 94 p. papunktis.
6. Jeigu pirmojo inkremento tikslas pasiektas, PO sumoka Tiekėjui 20% (dvidešimt procentų) nuo Tiekėjo pasiūlyme nurodytos pirkimo objekto dalies „AP sukūrimo, modernizavimo ir diegimo paslaugos“ kainos Sutartyje nustatyta tvarka.
7. Tolesnių inkrementų ir iteracijų tikslų, apimties, detalių reikalavimų, kalendorinių terminų ir papildomų ekspertinių paslaugų planavimas vykdomas glaudžiai bendradarbiaujant Tiekėjui ir PO inkrementų planavimo renginių eigoje (žr. aukščiau).
8. Sekantys inkrementai apmokami paslaugų Sutartyje nustatyta tvarka pagal faktiškai Tiekėjo atliktus ir PO priimtus darbus, neviršijant tam inkrementui skirtos pirkimo objekto “AP sukūrimo, modernizavimo ir diegimo paslaugos” dalies vertės procentinės dalies, po kiekvieno inkremento priėmimo - perdavimo akto pasirašymo (Žr. Reikalavimas Nr. 103).
9. Esant esminiams tolesnių nei pirmas inkrementas rezultatų trūkumams, PO turi teisę reikalauti esminių trūkumų pašalinimo Tiekėjo sąskaita per terminą, kuris neturi viršyti 1 mėn. nuo suplanuoto inkremento termino, ir apmoka anksčiau suderintą inkremento sąmatą (Žr. Reikalavimas Nr. 103) tik pasirašius inkremento priėmimo-perdavimo aktą paslaugų Sutartyje nustatyta tvarka.
10. Tiekėjui nepašalinus esminių tolesnio nei pirmas inkremento trūkumų per nustatytą terminą, PO turi teisę nutraukti Sutartį, atlyginus tik už kokybiškai atliktus inkremento plane numatytus darbus tokia tvarka:
    1. PO sutartu būdu patvirtina kokybiškai atliktų inkremento plano darbų sąrašą,
    2. Pagal PO patvirtintus kokybiškus inkremento dalies darbus, Tiekėjas įvertina jų kainą pagal savo ekspertų, atlikusių šiuos darbus, darbo valandas, paslaugų Sutartyje nustatyta tvarka pateikia PO paslaugų perdavimo - priėmimo aktą,
    3. Už kokybiškai atliktus inkremento darbus atsiskaitoma paslaugų Sutartyje nustatyta tvarka. PO turi teisę visiškai nepriimti ir neapmokėti inkremento plano, jeigu nėra patvirtinta kokybiškai atliktų darbų,
    4. Nepriimtų ir neapmokamų darbų išeities kodas ir kiti artefaktai pašalinami iš PO GIT ir nebus panaudoti.
11. Jeigu faktinės Tiekėjo sąnaudos viršija pirkimo objekto dalies „AP sukūrimo, modernizavimo ir diegimo paslaugos“ pasiūlymo kainą, tuomet tai traktuojama, kaip Tiekėjo rizika ir neturi būti kompensuojama iš PO pusės.
12. Tiekėjas turi užtikrinti Perkančiajai organizacijai visišką išeities kodo, projektinių užduočių ir darbų eilės (angl. backlog), darbų eigos skaidrumą, tiesioginį bendradarbiavimą, įsitraukimą į įgyvendinimo darbus, naudojant PO suteiktas GIT priemones (žr. Reikalavimai išeities kodo ir darbų valdymui).
13. Lentelėje pateikiama AP sukūrimo, modernizavimo ir diegimo paslaugos etapų terminai bei atsiskaitymų dalys:

|  |  |  |  |
| --- | --- | --- | --- |
| **Inkremento Nr.** | **Inkremento apimtis** | **Numatytas vykdymo terminas** | **Atsiskaitymų dalys** |
| 1 inkrementas | Aprašyta reikalavime Nr. 94. | Ne vėliau kaip 2 mėnesiai nuo sutarties įsigaliojimo datos | **20%** nuo pirkimo objekto dalies “AP sukūrimo, modernizavimo ir diegimo paslaugos” vertės. |
| 2 inkrementas | Tapatybės nustatymas integracijos su visais bankais, išvardintais reikalavime Nr. 11.3.1.1, būdu.  Tapatybės nustatymas mobilaus parašo būdu.  Tapatybės nustatymo operacijų audito žurnalas.  Sąveika su bandomosios Institucijos IS simuliatoriumi V2 protokolu.  Pašalinti suderinti ankstesnio inkremento neesminiai trūkumai. | Ne vėliau kaip 4 mėnesiai nuo sutarties įsigaliojimo datos | **20%** nuo pirkimo objekto dalies “AP sukūrimo, modernizavimo ir diegimo paslaugos” vertės. |
| 3 inkrementas | Pilnai įgyvendinti VI.4 „Integracijos su išorinėmis autentifikavimo sistemomis“ skyriaus reikalavimai.  Atstovavimo pagal JAR funkcionalumas ir atstovavimo operacijų audito žurnalas.Pašalinti suderinti ankstesnių inkrementų neesminiai trūkumai. | Ne vėliau kaip 6 mėnesiai nuo sutarties įsigaliojimo datos | **20%** nuo pirkimo objekto dalies “AP sukūrimo, modernizavimo ir diegimo paslaugos” vertės. |
| 4 inkrementas | Visi Techninės specifikacijos reikalavimai įgyvendinti pilna apimtimi.  Pašalinti suderinti ankstesnių inkrementų neesminiai trūkumai. | Ne vėliau kaip 9 mėnesiai nuo sutarties įsigaliojimo datos | **40%** nuo pirkimo objekto dalies “AP sukūrimo, modernizavimo ir diegimo paslaugos” vertės. |

## VII.2 Reikalavimai išeities kodo ir darbų valdymui

1. Tiek teikiant sukūrimo, modernizavimo ir diegimo paslaugas, tiek teikiant garantinės priežiūros ir palaikymo paslaugas, visas AP išeities kodo bei kiti technologinių artefaktų pakeitimai turi būti saugomi ir tvarkomi PO naudojamoje išeities kodo ir versijų valdymo platformoje (PO GIT) ne rečiau nei vieną kartą per savaitę.
2. AP kūrimo ir palaikymo darbų eilė (angl. backlog) turi būti tvarkomos PO GIT, užduotys turi būti rišamos su išeities kodo saugyklomis (angl. repositories) ir versijomis (angl. branches).
3. PO GIT turi būti teikiami taip pat visos trečiųjų šalių ir/ar atviro kodo komponentai ir jų versijų atnaujinimai, reikalingi sėkmingam programinės įrangos sukompiliavimui ir įdiegimui.
4. Pateikiamas išeities kodas turi atitikti gerąsias praktikas pagal Programinio išeities kodo kokybės užtikrinimo standartą (ISO/IEC 25010:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models).
5. Projekto eigoje Tiekėjas turi automatizuoti PO GIT išeities kodo versijų kompiliavimo ir testavimo procesus PO GIT platformoje bei integruoti su VITC naudojamomis versijų kontrolės ir diegimo automatizuotomis priemonėmis.

## VII.3. Reikalavimai dokumentacijai

1. Projekto apimtyje pagal Šalių suderintą inkrementų planą Tiekėjas turi parengti, palaikyti ir naujinti **technines** **specifikacijas**:
   1. AP specializuotos programinės įrangos komponenčių architektūros specifikacija,
   2. AP diegimo aplinkų specifikacija,
   3. AP duomenų bazių struktūros specifikacija,
   4. Kiekvienos išorinės integracijos programinių sąsajų, protokolų, formatų specifikacija.
2. Projekto eigoje Tiekėjas turi bendradarbiauti su VIISP priežiūros tiekėju ir padėti parengti VIISP TNP demontavimo ir VIISP integracijos su AP specifikaciją. Už šios specifikacijos parengimą atsakingas VIISP priežiūros tiekėjas.
3. Projekto apimtyje pagal Šalių suderintą inkrementų planą Tiekėjas turi parengti, palaikyti ir naujinti **metodinę dokumentaciją**:
   1. Integracijos su AP specifikacija, skirta institucijoms ir jų tiekėjams pagal VIISP TNP pavyzdį (<https://www.epaslaugos.lt/portal/content/1257>), įskaitant pavyzdines realizacijas (angl. reference implementation), kuriomis būtų galima išbandyti autentifikavimo paslaugos veikimą iš Institucijos IS pusės (prisijungimą, perjungimą, SSO (single sign on) funkcijas ir kita sąveikumą),
   2. AP operacijų ir klaidų žurnalo analizės dokumentacija, skirta VSSA personalui, įskaitant rekomendacijas dėl statistikos skaičiavimo ir duomenų analitikos priemonių taikymo,
   3. AP stebėsenos dokumentacija, skirta VSSA / VITC darbuotojams, įskaitant rekomendacijas dėl Zabbix, IBM QRadar SIEM ir GrayLog priemonių integracijos, rodiklių, perspėjimų (angl. alert).
4. Visa dokumentacija turi būti rengiama laikantis bendrinės lietuvių kalbos taisyklių.
5. Visos dokumentacijos galutinės versijos turi būti pateikiamos PO GIT ir suderintos / patvirtintos PO.

## VII.5 Reikalavimai priėmimo testavimui

1. Galutinio inkremento rezultatų priėmimo testavimo metu (ar kitu sutartu atveju) Tiekėjas turi sudaryti visas reikiamas sąlygas PO atstovų ir tiekėjų specialistams atlikti tiek funkcinius, tiek nefunkcinius AP testus:
   1. Apkrovos,
   2. Atsparumo įsilaužimams ir kitą saugos testavimą,
   3. Išeities kodo analizę,
   4. Dokumentacijos pilnumo ir korektiškumo testavimą.
2. Esant poreikiui Tiekėjas turės atlikti konfigūravimo ar programavimo darbus, būtinus AP saugumo testavimui ir/arba testavimo metu pastebėtų trūkumų ir rizikų šalinimui.
3. Visi priėmimo testavimo metu pastebėti trūkumai ir klaidos turi būti šalinamos Tiekėjo sąskaita terminais, aprašytais sk. [VII.1 Reikalavimai įgyvendinimo būdui ir paslaugų teikimo etapams](#_VII.1_Reikalavimai_įgyvendinimo).

**VII.6 Reikalavimai garantinės priežiūros ir palaikymo paslaugoms**

1. Garantinio palaikymo paslaugos turi būti įskaičiuotos į sukūrimo ir diegimo kainą ir turi būti teikiamos 12 (dvylika) mėnesių termino laikotarpiu po paskutinio inkremento įdiegimo priėmimo-perdavimo akto pasirašymo dienos.
2. Paslaugos Teikėjas garantinio laikotarpio metu privalo turėti tinkamos kvalifikacijos specialistus, kad būtų užtikrintas garantinių Paslaugų teikimas per Sutartyje nustatytą laiką.
3. Garantiniu laikotarpiu atliekami darbai negali sugadinti veikiančio ir nekeičiamo AP funkcionalumo ar kitų integruotų informacinių sistemų darbo.
4. Garantinės priežiūros paslaugos apima:
   1. Paslaugų teikimo metu modifikuotus ir/ar sukurtiems AP komponentus ir kitas AP naudojamas technologijas, kurias pasiūlė ir įdiegė Tiekėjas,
   2. AP integracijas su kitomis informacinėmis sistemomis ir priemonėmis, išskyrus tuos atvejus, kai neplanuojamas pokytis įvyksta integruotoje sistemoje ir nepriklauso nuo Tiekėjo veiksmų,
   3. Sugadintų ar prarastų AP ir/ar kitų suintegruotų informacinių sistemų duomenų atstatymą, kai gedimas įvyko dėl Tiekėjo kaltės, pavyzdžiui, dėl Tiekėjo pateiktos ir įdiegtos versijos (programinė įranga, sukurta duomenų bazė, įdiegta technologija ir pan.) netinkamo veikimo arba neveikimo,
   4. AP programinės įrangos ar jos terpėje naudojamų technologijų saugos pažeidžiamumams.
   5. PO konsultavimą AP plėtros, diegimo, integracijos klausimais arba sprendžiant integruotų informacinių sistemų gedimus, kurie įvyko ne dėl Tiekėjo kaltės. Konsultacijos neturi viršyti 16 val. per kalendorinį mėnesį.
5. Garantija nustoja galioti esant bent vienai iš šių sąlygų:
   1. Nuo priėmimo-perdavimo akto pasirašymo dienos praeina 12 mėnesių,
   2. AP veikimo stebėjimas, priežiūra ir modifikavimas perduodama naujam Teikėjui,
   3. AP gamybinėje aplinkoje diegiami ne Teikėjo parengti programinės įrangos pakeitimai.

# VII SKYRIUS: PRIEDAI

1. Priedas 1. Tapatybės nustatymo modulio specifikacija (<https://www.epaslaugos.lt/portal/file/af0c4396-817a-4de8-b75b-ee7fc5801e28>).
2. Priedas 2. Naujas Web dizainas (ZIP failas)
3. Priedas 2. VIISP autentifikacijos konfigūraciniai parametrai ir naudojami duomenys.
4. Priedas 3. El. paslaugų naudotojo/atstovaujamo ir atstovaujančiojo asmens duomenų perdavimas į išorę V2 protokolu.