Specialiųjų sąlygų 2 priedas „Techninė specifikacija“

# Prieigos taško EESSI AP (access point) priežiūros paslaugos

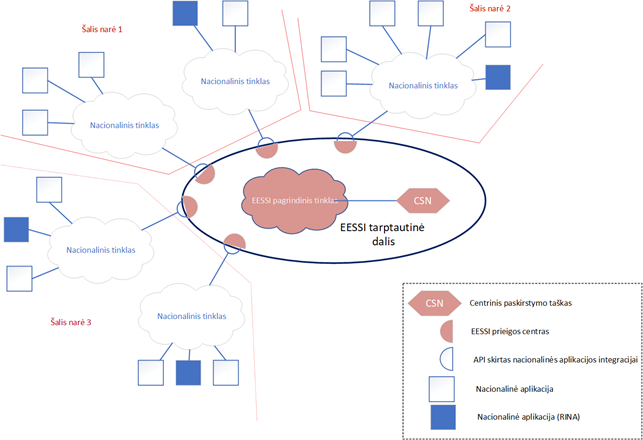
# TECHNINĖ SPECIFIKACIJA

1. PIRKIMO OBJEKTAS
   1. Elektroninio apsikeitimo socialinės apsaugos informacija EESSI (*Electronic exchange of social security information)* tarp ES valstybių narių ir Lietuvos nacionalinio prieigos taško (centro) (toliau – *access point* /AP) priežiūros paslaugos (toliau – paslaugos), apimančios ir būtinas *access point* (AP) naujinimo, naudotojų konsultavimo ir kitas susijusias paslaugas, atitinkančias šios techninės specifikacijos reikalavimus.
   2. Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos (toliau – Užsakovas) planuoja įsigyti *access point* (AP) priežiūros paslaugas 12 (dvylikos) mėnesių laikotarpiui, su galimybe jį pratęsti du kartus po 12 mėnesių, neviršijant bendro 36 mėnesių AP viešojo pirkimo sutarties laikotarpio.
2. BENDROSIOS SĄLYGOS
   1. Išorinis paslaugų teikėjas, teikdamas paslaugas privalės vadovautis:
      1. Valstybės informacinių išteklių valdymo įstatymu, patvirtintu, Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 1 d. nutarimu Nr. 907 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo“;
      2. Informacinių technologijų paslaugų valdymo metodika, patvirtinta Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. birželio 19 d. įsakymu Nr. T-83 „Dėl informacinių technologijų paslaugų valdymo metodikos patvirtinimo“;
      3. Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, patvirtinta Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014 m. vasario 25 d. įsakymu Nr. T-29 „Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo“;
      4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos Reglamentu (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/BDAR).
   2. Nuosavybės teisės bei visos autorių turtinės teisės į Išorinio paslaugų teikėjo paslaugų teikimo sutarties vykdymo metu sukurtą programinę įrangą, įskaitant programinės įrangos išeities kodą, ir dokumentus pereina Užsakovui nuo paslaugų priėmimo–perdavimo akto pasirašymo datos.
   3. Paslaugų teikimo metu Išorinis paslaugų teikėjas privalės derinti veiksmus ir sprendimus su Pirkimo sutarties vykdymo laikotarpiu vykstančiais kitais projektais, vykdomais pagal kitas sutartis, Užsakovo informacinių technologijų techninės ir technologinės infrastruktūros pokyčiais bei kitų Užsakovo informacinių sistemų plėtra.
3. ESAMOS SITUACIJOS APRAŠYMAS
   1. Naudojamos sąvokos ir trumpiniai:

1 lentelė. *Terminų ir trumpinių paaiškinimas*

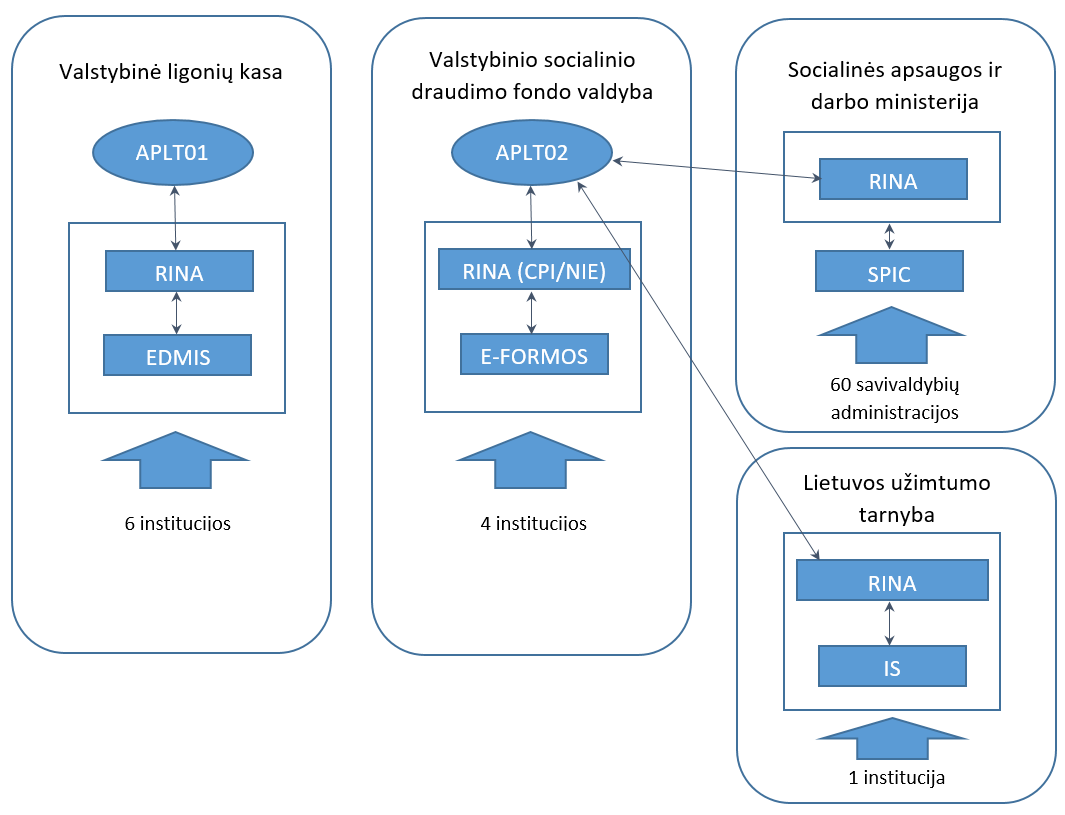
|  |  |
| --- | --- |
| **Santrumpa** | **Paaiškinimas** |
| Prieigos centras (taškas) (angl. *access point*, AP) | Prieigos centras skirtas pranešimų keitimuisi tarpvalstybiniame lygmenyje. Jis jungia EESSI europinę ir nacionalinę dalis. Kiekviena valstybė narė turi iki 5 prieigos centrų. Kiekviena atskira kompetentinga įstaiga turi tiesioginį ryšį su konkrečiu valstybės prieigos centru, per kurį elektroniniai pranešimai siunčiami kitos valstybės narės kompetentingai įstaigai. |
| API | Programinė sąsaja. |
| BUC | Veiklos atvejis (*angl. Business use case*), taisyklių rinkinys, tiksliai apibrėžiantis, kokiais pranešimais ir kokiu eiliškumu turės būti keičiamasi kiekvienu informacijos apsikeitimo tarp valstybių atveju.  Kiekvienas BUC turi unikalų ID bei rinkinį SED. |
| CSN | Tai EESSI europinės dalies centrinis mazgas, kuris skirtas užtikrinti komunikaciją tarp valstybių narių prieigos centrų, per ICD1 sąsają. |
| CPI | *Case processing services interface, web service* sąsaja, skirta institucijų sistemų integracijai su RINA, skirta perduoti duomenis iš institucijų sistemų į konkretų RINA atvejų apdorojimo modulį. |
| EESSI | Elektroninių socialinės apsaugos informacijos mainų sistema (angl*. Electronic Exchange of Social Security Information*) kaip numatyta 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamente (EB) Nr. 883/2004 dėl socialinės apsaugos sistemų koordinavimo ir 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos reglamente (EB) Nr. 987/2009, nustatančiame Reglamento Nr. 883/2004 dėl socialinės apsaugos sistemų koordinavimo įgyvendinimo tvarką. |
| Nacionalinė aplikacija | Funkcinis EESSI sistemos komponentas, priklausantis nacionalinei EESSI sistemos daliai, užtikrinantis EESSI sistemos integraciją su konkrečia socialinės apsaugos institucija. |
| NIE | *National Information Exchange Interface, web service* sąsaja, skirta institucijų sistemų integracijai su RINA, skirta gauti duomenis iš RINA atvejų apdorojimo modulio į institucijų sistemas. |
| RINA | EESSI sistemos įrankis, skirtas duomenų mainams su Europos Sąjungos valstybių nacionalinėmis sistemomis (angl. *Reference Implementation of a National Application*). Ši programinė įranga skirta rengti ir siųsti SED per valstybės narės AP.  RINA sudaro trys atskiros dalys: *transporto dalis*, apimanti SED siuntimo ir gavimo procesus ir taisykles, *veiklos dalis*, apimanti BUC procesų aprašymą ir kitas veiklos procedūras, ir *naudotojo sąsaja*. |
| SED | Struktūrizuotas elektroninis dokumentas (angl. *Structured Electronic Document*), tam tikros struktūros dokumentas, pateikiamas ES valstybių narių tarpusavio elektroniniu keitimuisi informacija nustatyta forma, kaip apibrėžta Reglamento (EB) Nr. 987/2009 1 straipsnio 2 dalies d punkte. |
| VLK | Valstybinė ligonių kasa |
| TLK | Teritorinė ligonių kasa (po 2025-07-01 įvykus konsolidavimo procedūrai, teritorinės ligonių kasos prijungiamos prie VLK ir taps vienu juridiniu asmeniu) |
| Web service (WS) | Technologija leidžianti dviem sistemoms bendrauti tarpusavyje per pasaulinį tinklą (angl. *World Wide Web*). |
| XML | W3C rekomenduojama bendros paskirties duomenų struktūrų ir jų turinio aprašomoji kalba. |
| IR | EESSI tinkle dalyvaujančių institucijų repozitorija. |
| ES VN | Europos sąjungos valstybės narės |
| Valstybės narės | Europos Sąjungos valstybės narės, Europos ekonominės erdvės valstybės, Šveicarija ir Jungtinė Karalystė. |

* 1. Europos Sąjungoje (toliau – ES) migruojančių asmenų socialinę apsaugą reglamentuoja ES socialinės apsaugos sistemų koordinavimo reglamentai. Nuo 2010 m. gegužės 1 d. įsigaliojo nauji ES socialinės apsaugos sistemų koordinavimo reglamentai, t. y. 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 883/2004 dėl socialinės apsaugos sistemų koordinavimo ir 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 987/2009, nustatantis Reglamento (EB) Nr. 883/2004 dėl socialinės apsaugos sistemų koordinavimo įgyvendinimo tvarkos (toliau – koordinavimo reglamentai).
  2. Koordinavimo reglamentuose yra numatytas perėjimas nuo keitimosi popieriniais dokumentais prie elektroninio apsikeitimo informacija. Pasibaigus pereinamajam laikotarpiui, valstybės narės socialinės apsaugos srityje privalės tarpusavyje keistis informacija elektroninėmis priemonėmis. Tai bus daroma per elektroninių socialinės apsaugos informacijos mainų sistemą (toliau – EESSI), siunčiant struktūrizuotus elektroninius dokumentus (toliau – SED).
  3. EESSI sistema skirta valstybių narių kompetentingų įstaigų specialistams, skiriantiems socialinės apsaugos išmokas pagal koordinavimo reglamentus.
  4. SED apsikeitime per EESSI dalyvauja visos ES valstybės narės, Europos ekonominės erdvės valstybės ir Šveicarija ir Jungtinė Karalystė (toliau kartu – valstybės narės).
  5. EESSI sudaro europinė ir nacionalinės dalys. Valstybių narių socialinės apsaugos įstaigos jungiasi prie EESSI sistemos per prieigos centrus (angl. *Access point*). Europos Komisija sukūrė europinę EESSI sistemos dalį, o valstybės narės yra atsakingos už nacionalinės dalies sukūrimą ir priežiūrą.
  6. Lietuvos Respublikos socialinės apsaugos ir darbo ministerija (toliau – SADM), Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos (toliau – Fondo valdyba) ir Užimtumo tarnyba prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos (toliau – Užimtumo tarnyba), prie EESSI sistemos prisijungė nuo 2019 m. liepos mėn. Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos (toliau – VLK) prie EESSI sistemos prisijungė nuo 2020 m. kovo mėn.
  7. EESSI tinklas yra kertinis elementas įgyvendinant koordinavimo reglamentus. EESSI projektas pradėtas įgyvendinti 2007 m., kuomet buvo atlikta optimalios sprendimo architektūros galimybių studija. Principinė EESSI tinklo architektūra pateikta paveiksle žemiau.



*1 paveikslas. EESSI principinė architektūra*

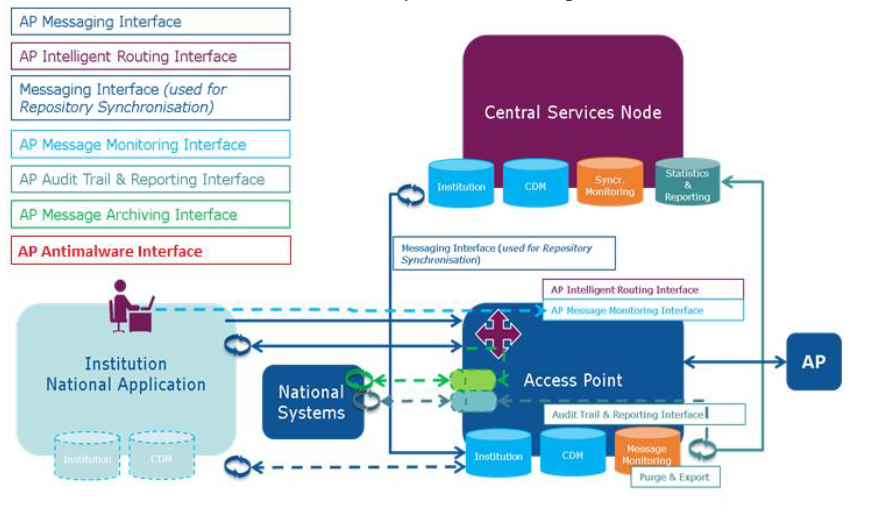
* 1. EESSI sudaro dvi pagrindinės sistemos dalys: tarptautinė ir nacionalinė dalys.
  2. Europinės sistemos lygmens komponentai yra bendri visoms valstybėms narėms. Už šią sistemos dalį yra atsakinga Europos Komisija. Yra išskiriamos atskiros šios dalies sritys:
     1. centrinis paskirstymo mazgas (angl. *EESSI Central Service Node – CSN*) – centrinė saugykla, kurioje centralizuotai bus saugoma informacija, skirta pranešimų maršrutui nustatyti. Komunikacija su šiuo mazgu galima tik per valstybių narių prieigos taškus;
     2. prieigos centras (taškas) (angl. *access point –* AP) – sritis, kuriai priklauso bendri visoms valstybėms narėms komponentai, tačiau šis komponentas bus konfigūruojamas kiekvienoje valstybėje narėje. Prieigos centrai užtikrina komunikaciją tarp tarptautinės ir nacionalinių sistemų dalių.
  3. Nacionalinė EESSI sistemos dalis:
     1. Nacionalinės aplikacijos – tai konkrečių institucijų veikloje naudojama programinė įranga, kuri užtikrina pranešimų siuntimą ir gavimą per EESSI.
  4. Lietuvos nacionalinės EESSI dalies principinė schema pateikta 2 paveiksle žemiau. Taip pat planuojama, kad bus įgyvendinamas Valstybinės ligonių kasos APLT01 (nuo 2025 m. liepos 1 d.) institucijų konsolidavimo pokytis, po kurio vietoj 6 institucijų liktų 1 juridinis asmuo.



2 paveikslas. *Lietuvos nacionalinės EESSI dalies principinė schema*

* 1. Lietuvoje prie EESSI infrastruktūros yra prijungtos 4 nacionalinės aplikacijos: SADM, Fondo valdybos, Užimtumo tarnybos, VLK. Kiekvienoje iš šių institucijų yra įdiegta RINA programinė įranga, kuri per integracines sąsajas yra integruota su vidinėmis institucijų sistemomis.
  2. Lietuvoje veikia du EESSI prieigos centrai: APLT01 – Valstybinėje ligonių kasoje, APLT02 – Fondo valdyboje. SADM, Fondo valdyba ir Užimtumo tarnyba jungiasi prie EESSI per APLT02 prieigos centrą. VLK ir teritorinės ligonių kasos jungiasi prie EESSI per APLT01 prieigos centrą.
  3. Kiekviena valstybė narė prie EESSI sistemos jungiasi palaipsniui pagal atskirus informacijos apsikeitimo atvejus (angl. *Business Use Case*, toliau – BUC). Valstybės narės, kurios yra prisijungusios prie EESSI sistemos dėl konkretaus BUC, dėl šio BUC privalo tarpusavyje keistis informacija tik elektroninėmis priemonėmis. Lietuvos kompetentingos įstaigos prie EESSI sistemos yra prisijungusios su visais 99 BUC.
  4. VLK išvykstančių į Europos Sąjungos šalis Lietuvos Respublikos apdraustųjų ir į Lietuvos Respubliką atvykusių Europos Sąjungos apdraustųjų duomenims tvarkyti naudoja savo kuriamą ir palaikomą Europos Sąjungos socialinės apsaugos duomenų mainų informacinę sistemą (toliau – EDMIS).
  5. Integracijai tarp RINA ir EDMIS yra naudojamos RINA CPI/NIE sąsajos (transporto dalis + veiklos dalis). Naudojant šią sąsają, EDMIS nereikia galvoti apie SED/BUC siuntimo (transporto) taisykles bei tarptautinės veiklos (verslo) taisykles, kurias kontroliuoja RINA centralizuotai. Transporto taisykles apima integracija su nacionaliniu prieigos centru, sertifikatų tvarkymą tiek su Lietuvos, tiek su užsienio prieigos taškais bei institucijomis, transportuojamo dokumento saugumo reikalavimų atitikimą bei sėkmingą dokumento pristatymą/gavimą. Taip pat naudojantis CPI/NIE sąsaja, užtikrinama, kad EDMIS nepateiktų į kitas įstaigas/šalis BUC ar SED, kurie neatitinka EESSI sistemos reikalavimų.
  6. Nors ir naudojama RINA CPI/NIE integracija, VLK turi įdiegusi pilną RINA versiją su naudotojo sąsaja rečiau naudojamiems BUC. Dėl kitų BUC yra įdiegta nacionalinė aplikacija EDMIS, kuri naudoja tik RINA transporto ir veiklos dalis.
  7. VLK įdiegta pilna RINA versija naudojasi 6 institucijos: VLK, Vilniaus TLK, Kauno TLK, Klaipėdos TLK, Šiaulių TLK, Panevėžio TLK.

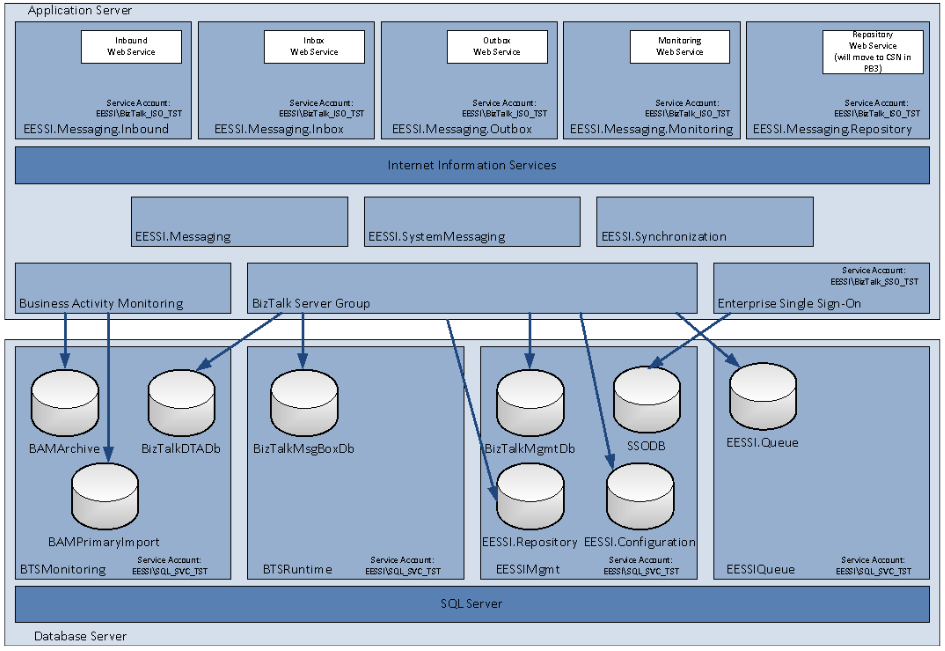
1. AP LOGINĖ ARCHITEKTŪRA
   1. Visa komunikacija tarp skirtingų institucijų EESSI tinkle vyksta per AP, panaudojant ebMS/AS4 protokolą per HTTPS.
   2. AP suteikia šias esmines funkcionalumų grupes:
      1. Žinučių siuntimas ir gavimas – tai viena iš kertinių AP funkcijų, kuri užtikrina elektroninių žinučių siuntimą ir gavimą laikantis EESSI žinučių formatų ir saugumo standartų;
      2. Institucijų repozitorijos (IR) sinchronizavimas – šis funkcionalumas užtikrina institucijų repozitorijos parsiuntimą iš CSN ir perdavimą į nacionalines aplikacijas;
      3. Žinučių siuntimo ir gavimo statistikos ir audito įrašų kaupimas;
      4. Žinučių archyvavimas;
      5. Sistemos monitoringas;
      6. Autentifikavimas ir autorizavimas – užtikrina prieigos teisių suteikimą ir valdymą AP portalo naudotojams;
      7. Audito žurnalas – užtikrina AP vykstančių funkcinių ir techninių procesų žurnalizavimą. Audito žurnalo paieškos ir peržiūros funkcionalumas leidžia identifikuoti AP aplikacijos klaidas.
   3. Žemiau esančiame paveiksle vaizduojami pagrindiniai AP loginės architektūros komponentai ir jų komunikacija su kitais EESSI tinklo komponentais:



3 paveikslas. *AP loginės architektūros komponentai ir jų komunikacija su kitais EESSI tinklo komponentais*

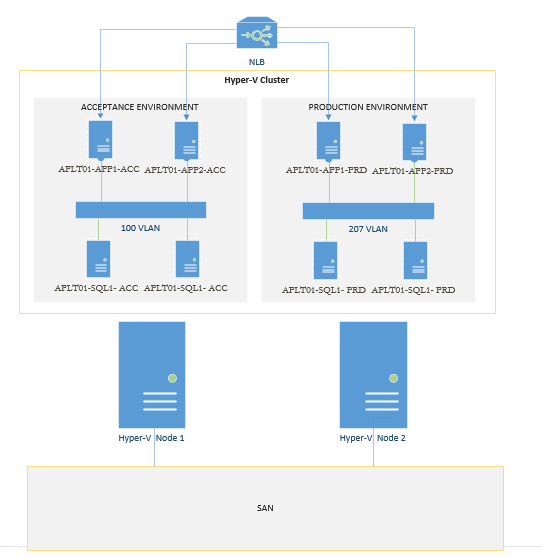
* 1. Esminiai AP loginės architektūros komponentai:
     1. AP pranešimų siuntimo komponentas (angl. *AP Messaging Interface*) – užtikrina veiklos pranešimų apsikeitimą tarp kompetentingų institucijų skirtingose ES šalyse bei sisteminių pranešimų (IR sinchronizavimas, audito žurnalo perdavimas ir pan.) apsikeitimą su CSN. Pranešimais yra keičiamasi naudojant ebMS AS4 protokolą, kuris užtikrina interoperabilumą, klaidų apdorojimą, saugumą ir patikimumą. Saugumo užtikrinimui naudojamas TLS, AS4 žinučių pasirašymas bei žinučių šifravimas.
     2. AP maršrutizavimo komponentas (angl. *AP Intelligent Routing Interface*) – suteikia galimybę sukonfigūruoti specifines pranešimų maršrutizavimo taisykles gaunančiame AP. Pastaba! APLT01 šis funkcionalumas šiuo metu nenaudojamas.
     3. IR sinchronizavimo pranešimų komponentas (angl. *Messaging Interface (used for Repository Synchronisation)*) – užtikrina lokalios AP repozitorijos sinchronizavimą su CSN. Sinchronizavimui taip pat naudojamas ebMS AS4 protokolas. IR repozitorijos duomenys iš CSN į AP yra perduodami kaip XML failas, o CDM duomenų modelio duomenys perduodami kaip zip archyvo failai.
     4. AP pranešimų monitoringo komponentas (angl. *AP Message Monitoring Interface*) – suteikia galimybę kaupti ir analizuoti informaciją apie pranešimų apsikeitimą AP. Kaupiami audito įrašai apie kiekvieną per AP persiunčiamą pranešimą (būsenos, pranešimų tipai, siuntėjas, gavėjas ir pan.), suteikiama galimybė atlikti paiešką bei peržiūrėti audito įrašus.
     5. AP audito žurnalo komponentas (angl. *AP Audit Trail & Reporting interface*) – perduoda agreguotą audito žurnalo informaciją į CSN.
     6. AP pranešimų archyvavimo komponentas (angl. *AP Message Archiving Interface*) – suteikia galimybę konfigūruoti archyvavimo taisykles bei nacionalinėms aplikacijoms gauti informaciją apie archyvuojamus pranešimus. Pats pranešimų archyvavimas nėra atliekamas AP.
     7. AP antivirusinis komponentas (angl. *AP Antimalware Interface*) – užtikrina, kad persiunčiami pranešimai (SED ir jų priedai) būtų skenuojami antivirusinės programinės įrangos. Pastaba! APLT01 šis funkcionalumas šiuo metu nenaudojamas.

1. AP TECHNOLOGINĖ ARCHITEKTŪRA
   1. AP pagrindą sudaro *BizTalk Server 2016 R2* ir *Microsoft SQL Server* programinė įranga.
   2. Žemiau esančiame paveiksle pavaizduotos AP BizTalk serverio aplikacijos ir duomenų bazės:



4 paveikslas. *AP BizTalk serverio aplikacijos ir duomenų bazės*

1. AP DIEGIMO ARCHITEKTŪRA
   1. Žemiau esančiame paveiksle pateikta VLK APLT01 diegimo schema:



5 paveikslas. *APLT01 diegimo infrastruktūra*

**BizTalk serveriai**

|  |  |  |
| --- | --- | --- |
| **Parametras** | **PROD aplinka** | **ACC aplinka** |
| **Tipas** | Virtualus | Virtualus |
| **Serverių kiekis** | 2 vnt. | 2 vnt. |
| **OS** | Windows Server 2016 Standard | Windows Server 2016 Standard |
| **PĮ** | BizTalk Server Enterprise Edition 2016 | BizTalk Server Enterprise Edition 2016 |

**DB serveriai**

|  |  |  |
| --- | --- | --- |
| **Parametras** | **PROD aplinka** | **ACC aplinka** |
| **Tipas** | Virtualus | Virtualus |
| **Serverių kiekis** | 2 vnt. | 2 vnt. |
| **OS** | Windows Server 2016 Standard | Windows Server 2016 Standard |
| **Sisteminė PĮ** | SQL Server 2016 Standard Edition | SQL Server 2016 Standard Edition |

1. REIKALAVIMAI GARANTIJAI IR PRIEŽIŪROS PASLAUGOMS
   1. Paslaugoms, t. y. paslaugų teikimo sutarties metu suteiktoms paslaugoms, turi būti suteikta 12 (dvylikos) mėnesių garantija. Garantija įsigalioja ir garantinė priežiūra teikiama be papildomo užmokesčio.
   2. Visiems paslaugų rezultato elementams (sudėtinėms dalims, pagal Civilinį kodeksą), kuriems pagal Civilinį kodeksą būtų galimybė sutartiniu įsipareigojimu suteikti kokybės garantijos terminą, paslaugų teikimo sutartimi suteikiamas 12 (dvylikos) mėnesių kokybės garantijos terminas, kurio pradžia laikoma perdavimo–priėmimo akto pasirašymo diena. Kokybės garantija turi būti taikoma:
      1. AP komponentų tarpusavio apjungimo, diegimo paslaugoms;
      2. Bet kokiems įsikišimams į programinės įrangos ir/ar atskirų jos elementų sandarą, kurie galėtų įtakoti (pakeisti, sutrikdyti) informacinės sistemos ir/ar jos elementų veikimą, turėtų įtakos programinės įrangos ir/ar jos elementų funkcionavimui, tikslumui, saugumui, kokybei, tinkamumui, integracijai, naudotojo darbui su programine įranga ir/ar jos elementais, neigiamai paveiktų (sugadintų, sunaikintų, sumažintų saugumą) programoje sukauptus ir saugomus bei naujai įvedamus duomenis ir informaciją, turėtų neigiamos įtakos (sutrikdytų, pakeistų) kitų, pagalbinių ir/ar nepriklausomų, programų bei programinės įrangos veiklai;
      3. Kokybės garantija apima sugadintų bei prarastų duomenų atstatymą, kai gedimo priežastis yra Išorinio paslaugų teikėjo įdiegtų priemonių netinkamas veikimas arba neveikimas;
      4. Išorinio paslaugų teikėjo atsakomybė už kokybės garantiją užtikrinama taip, kaip numato Civilinis kodeksas, t. y. nėra nustatyti jokie kiti Išorinio paslaugų teikėjo suteikiamos kokybės garantijos užtikrinimo ar atsakomybės už kokybės garantiją apribojimai. Kokybės garantijos termino eiga sustabdoma laikotarpiui nuo pranešimo apie Paslaugos rezultato elemento trūkumą iki tokio Paslaugos rezultato elemento trūkumo pašalinimo momento. Jeigu tam tikriems Paslaugos rezultato elementams Paslaugos rezultato elementų gamintojas standartiškai suteikia ilgesnį kokybės garantijos terminą, taikomas toks ilgesnis kokybės garantijos terminas. Kokybės garantiniai įsipareigojimai negali būti skaidomi į atskirus garantinius įsipareigojimus atskiriems funkciškai glaudžiai tarpusavyje susijusiems komponentams, kas taip pat reiškia, kad: baziniam funkcionalumui (moduliams, užtikrinantiems kitų modulių sąveiką, aprūpinantiems pastaruosius reikiama informacija, leidžiantiems valdyti kitų modulių funkcionavimą ir pan.) garantiniai įsipareigojimai taikomi ne trumpiau nei vėliausiai pasibaigiantys garantiniai įsipareigojimai priklausomiems moduliams (kad nesusidarytų situacija, kai garantiniai įsipareigojimai taikomi priklausomam elementui, kai tuo tarpu jo funkcionavimui būtinam elementui garantiniai įsipareigojimai netaikomi).
      5. Kokybės garantijos termino metu Išorinis paslaugų teikėjas, pagal gautą Užsakovo pranešimą, privalo savo lėšomis ir neatlygintinai pašalinti Paslaugų rezultato elementų (Išorinio teikėjo pateiktų ar sukurtų) trūkumus. Reakcijos ir neatitikimų šalinimo laikas turi būti toks, kad Paslaugos rezultatas galėtų dirbti realaus laiko režimu, kai to reikalaujama pagal AP specifikaciją. Jeigu Išorinis paslaugų teikėjas neatitikimų šalinimo procese neužtikrina Paslaugų rezultato darbo realaus laiko režimu, ir dėl to Užsakovas pašalina neatitikimus be Išorinio paslaugų teikėjo, su tuo susijusias Užsakovo išlaidas nedelsiant įsipareigoja padengti Išorinis paslaugų teikėjas.
   3. Garantijos laikotarpiu Išorinis paslaugų teikėjas pagal Užsakovo poreikį turės teikti pagalbą (techninę konsultaciją) visais įgyvendintų funkcinių sprendimų klausimais telefonu, elektroniniu paštu, susitikimo metu, lietuvių kalba Užsakovo sistemos naudotojams iš sistemos palaikymui numatytų valandų.
   4. Išorinis paslaugų teikėjas turės informuoti apie programinės įrangos gamintojo naujausią programinę įrangą ir jos versijas, reikalingus keitimus ir suderinęs laiką šiuos naujinimus sudiegti.
   5. Išorinis paslaugų teikėjas privalės pradėti šalinti sutrikimą ne vėliau kaip per 4 (keturias) Užsakovo darbo laiko valandas nuo pranešimo apie sutrikimą gavimo.
   6. Eksploatuojamos programinės įrangos darbingumo atstatymas turi būti užtikrintas per 6 darbo val. nuo sutrikimo šalinimo pradžios.
   7. Sutrikimo šalinimo trukmė privalės neviršyti 6 (šešių) Užsakovo darbo laiko valandų nuo pranešimo apie sutrikimą gavimo, jeigu sutrikimas nėra susijęs su standartiniu gamintojo funkcionalumu. Išskirtiniais atvejais, jei sutrikimo per nurodytą laiką pašalinti neįmanoma (pvz. jei reikalingos gamintojo programinės korekcijos ar panašiai), su Užsakovu suderinamas atskiras sutrikimo pašalinimo terminas.
   8. Sistemų dokumentacijos atnaujinimas, atsižvelgiant į atliktus sistemos pakeitimus, turi būti atnaujintas ir pateiktas Užsakovui per 10 dienų.
2. REIKALAVIMAI DUOMENŲ SAUGAI
   1. Išorinis paslaugų teikėjas, vykdydamas AP priežiūros paslaugas, turi atitikti nustatytus valstybės IS kūrimo, plėtros, vystymo, techninės priežiūros, asmens duomenų konfidencialumo, prieinamumo, vientisumo ir informacijos saugos reikalavimus ir vadovautis šios Techninės specifikacijos 2.1 punkte nurodytais teisės aktais ir:
      1. BDAR;
      2. Lietuvos Respublikos elektroninių ryšių įstatymu;
      3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;
      4. Lietuvos Respublikos kibernetinio saugumo įstatymu;
      5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu patvirtintu Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 12 d. nutarimu Nr. 945 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.
      6. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;
      7. Standartais LST ISO / IEC 27002, LST ISO / IEC 27001 arba lygiavertėmis informacijos saugą užtikrinančiomis priemonėmis;
      8. kitais duomenų saugą reglamentuojančiais Lietuvos Respublikos teisės aktais.
   2. Paslaugų teikimo sutarties sąlygas ir reikalavimus Išorinių paslaugų teikėjas privalės vykdyti vadovaudamasis duomenų saugą reglamentuojančių Užsakovo teisės aktų nuostatomis.
   3. Išoriniam paslaugų teikėjui neskelbtina informacija teikiama tik tokios apimties, kuri būtina Paslaugai atlikti. Išorinis paslaugų teikėjas turi pasirašyti duomenų teikimo sutartį su kiekviena institucija, o Teikėjo darbuotojai pasirašo duomenų konfidencialumo išsaugojimo pasižadėjimus. Išorinis paslaugų teikėjas turi imtis visų priemonių gautai informacijai apsaugoti, todėl Išoriniam paslaugų teikėjui nustatomi tokie pagrindiniai reikalavimai:
      1. neskleisti ir neperduoti kitiems fiziniams ar juridiniams asmenims iš Užsakovo gautos informacijos, užtikrinti tinkamą jos saugą, laikyti ją paslaptyje net pasibaigus ,Paslaugų teikimo sutarties galiojimui;
      2. Išorinis paslaugų teikėjas turi užtikrinti ir garantuoti, kad Išorinio paslaugų teikėjo darbuotojai, kurie atliks Paslaugą, saugos AP naudojamų duomenų paslaptį tiek Paslaugos teikimo metu, tiek perėjus dirbti į kitas pareigas, tiek pasibaigus Paslaugos sutarčiai, tiek pasibaigus Išorinio paslaugų teikėjo darbuotojų darbo ar kitokiems santykiams su Išoriniu paslaugų teikėju;
      3. apie informacijos paskleidimo ar perdavimo kitiems fiziniams ar juridiniams asmenims faktą nedelsiant raštu informuoti Užsakovą ir imtis visų būtinų veiksmų užkirsti kelią tolesniam informacijos paskleidimui;
      4. atlyginti dėl informacijos neteisėto paviešinimo kilusius nuostolius.
   4. Išoriniam paslaugų teikėjui prieiga prie AP aplinkų bei serverių suteikiama Užsakovo nustatyta tvarka.
   5. Visi informacinių sistemų naudotojų administravimo ir informacijos saugumo reikalavimai, taikomi Išoriniam paslaugų teikėjui, yra taikomi ir jo subrangovams.
   6. Siūlomi saugumo sprendimai turi atitikti Užsakovo teisės aktuose numatytus reikalavimus, susijusius su duomenų saugumu, bei užtikrinti Užsakovo infrastruktūros ir duomenų saugą.
3. REIKALAVIMAI VLK AP PRIEŽIŪROS PASLAUGOMS
   1. VLK AP priežiūros metu Išorinis paslaugų teikėjas turi teikti šias paslaugas:
      1. avarijų, kritinių situacijų, incidentų ir problemų sprendimas;
      2. AP veiklos bei sąsajų su kitomis sistemomis veikimo ir atsarginio kopijavimo stebėsena (*angl. monitoring*), Užsakovo prašymu spręsti stebėsenos metu pastebėtas problemas. AP administravimas, veikimo būsenos stebėsena bei iškilusių problemų sprendimas turi būti teikiamas vadovaujantis Europos Komisijos parengta AP administravimo ir priežiūros dokumentacija: *EESSI – AP Administration Manual, EESSI – AP Operations – Infrastructure Monitoring Guide, EESSI – AP – Operations – Security Guide*;
      3. Užsakovo naudotojų ir administratorių konsultavimas (lietuvių kalba) EESSI SED pranešimų siuntimo/gavimo sutrikimo atveju;
      4. atnaujinimų ir klaidų taisymo paketų diegimas, susijusios dokumentacijos atnaujinimas ir pateikimas. Naujų AP programinės įrangos versijų diegimas ir konfigūravimas turi būti teikiamas vadovaujantis Europos Komisijos parengta AP diegimo ir atnaujinimo dokumentacija: *EESSI – AP Installation and Configuration, EESSI – AP Installation and Configuration – Upgrade Guide*;
      5. prieigos prie techninės ir kitokio pobūdžio informacijos ir dokumentacijos suteikimas;
      6. sisteminių klasifikatorių, parametrų ir sertifikatų tvarkymas;
      7. ketvirtinių suteiktų priežiūros paslaugų (pagal pobūdį ir kiekį) ataskaitų teikimas;
      8. kas pusmetį pateikti IS prieinamumo ataskaitą;
      9. užtikrinti AP darbo atkūrimą visiško arba dalinio funkcionavimo sutrikimo atvejais, įskaitant sutrikimus, atsiradusius dėl klaidų programinėje įrangoje, ir dėl klaidų, atsiradusių dėl praradimų ir netikslumų duomenyse (pvz., techniškai sugadinti įrašai duomenų bazėje, dėl klaidingo programinės įrangos veikimo nekorektiškai suformuotas įrašo (-ų) turinys ir pan.). AP veikimo atstatymas visiško arba dalinio sutrikimo atvejais turi būti teikiamas vadovaujantis Europos Komisijos parengta AP rezervinio kopijavimo ir atstatymo dokumentacija: *EESSI – AP Operations – Backup and Disaster Recovery Guide*.
   2. Sutrikus AP darbui, iškilus sistemos taisymo ar papildymo, stebėsenos bei pagalbos techniniais ar funkciniais klausimais poreikiui, yra fiksuojamas įvykis (kreipinys), kuris gali būti kvalifikuojamas kaip sutrikimas, konsultacija.
   3. Apie AP pastebėtus sutrikimus yra pranešama Išoriniam paslaugų teikėjui naudojant Teikėjo Naudotojų aptarnavimo informacinę sistemą (toliau – NAT IS). Su sutrikimu susijęs susirašinėjimas ir sutrikimo sprendimo būdas turi būti pateikiami per NAT IS. Prie sutrikimo sprendimo būdo esant poreikiui turi būti pateikta nuoroda į naudotojo arba administratoriaus vadovą. Nepateikus tokios nuorodos sutrikimas turės būti grąžintas spręsti.
   4. Kiekvienam kreipinio tipui priskiriamas atitinkamas prioritetas. Kreipinio tipą ir prioritetą nustato Užsakovas. Išorinio paslaugų teikėjo siūlymu kreipinio tipas ir prioritetas gali būti tikslinami.
   5. **Kreipinio sprendimo laikas** – tai laikas nuo momento, kai registruotas kreipinys buvo pirmą kartą perduotas Išoriniam paslaugų teikėjui spręsti iki jo paskutinio sprendimo perdavimo VLK. Išorinio paslaugų teikėjo **reakcijos laikas** yra laikas, per kurį teikėjas praneša, kad gavo kreipinį.
   6. AP sutrikimų tipai, jų prioritetai, sprendimo bei reakcijos laikai pateikiami 2 lentelėje.

2 Lentelė. *Kreipinių tipai, jų prioritetai ir sprendimo bei reakcijos laikas:*

| **Kreipinio tipas** | |  | **Reakcijos trukmė, darbo val.** | **Išsprendimo trukmė, darbo val.** |
| --- | --- | --- | --- | --- |
| **Kreipinio klasifikacija** | **Prioritetas** | **Aprašymas** |
| Incidentas | I (Kritinis) | * visos AP funkcijos (įskaitant ir integracinių sąsajų sprendimus) neprieinamos arba veikia nekorektiškai, * AP atsakinti techniniai naudotojai negali prisijungti prie sistemos, * dėl sistemos funkcijų neveikimo yra iškilusi grėsmė sistemos duomenų korektiškumui ir vientisumui | 1 | 6 |
| Incidentas | II (Aukštas) | * viena arba dalis AP funkcijų (įskaitant ir integracinių sąsajų sprendimus) neprieinamos arba veikia kritiškai nekorektiškai, * nėra laikinų problemos sprendimo būdų, sistemos duomenų korektiškumui ir vientisumui grėsmės nėra, * AP atsakinti techniniai naudotojai negali atlikti pagrindinių sistemos operacijų | 2 | 10 |
| Incidentas | III (Vidutinis) | * viena arba dalis AP funkcijų (įskaitant ir integracinių sąsajų sprendimus) veikia nestabiliai arba reikalaujant automatizuotą procesą koreguoti rankiniu būdu, * sistemos duomenų korektiškumui ir vientisumui grėsmės nėra, * AP atsakinti techniniai naudotojai gali atlikti pagrindines sistemos operacijas | 2 | 18 |
| Incidentas | IV (Žemas) | * AP funkcija (integracinės sąsajos sprendimas) arba funkcijos elementas veikia nekorektiškai, * šis sutrikimas pagal poreikį išsprendžiamas rankiniu būdu, * sistemos duomenų korektiškumui ir vientisumui grėsmės nėra, * AP atsakinti techniniai naudotojai gali atlikti pagrindines sistemos operacijas | 2 | 38 |

* 1. Išorinis paslaugų teikėjas turi užtikrinti paslaugų lygį – incidentų išsprendimo ir reakcijos laikus. Paslaugų lygio užtikrinimas įeina į mėnesinį sistemos priežiūros mokestį.
  2. Jei incidento neįmanoma išspręsti per 2 lentelėje nurodytą išsprendimo trukmę, šalys gali susitarti dėl kitos incidento išsprendimo trukmės.
  3. Sutrikimas laikomas pašalintu, kai nustatyta tvarka pažymimi atitinkami įrašai NAT IS.
  4. Konsultavimas AP priežiūros klausimais turi būti teikiamas lietuvių kalba visą priežiūros laikotarpį telefonu, el. paštu, NAT IS, naudotojų darbo vietose ar kitais sutartais būdais darbo dienomis Užsakovo darbo valandomis. Taip pat Išorinis paslaugų teikėjas turi suprasti anglų kalba gaunamus dokumentus bei informaciją, skirtą bendravimui su ES institucijomis.
  5. Vykdant stebėseną ir pastebėjus kritinio arba aukšto tipo incidentą, Išorinis paslaugų teikėjas turi nedelsiant informuoti Užsakovą.
  6. Kitos sąlygos:
     1. Po kiekvieno išspręsto sutrikimo esant poreikiui, Išorinis paslaugų teikėjas, turės atnaujinti administratoriaus vadovus ir kitus sistemos dokumentus. Administratoriaus vadovai turi būti pateikiami tokio detalumo, kad sistemos administratorius be Išorinio paslaugos teikėjo konsultacijos gebėtų atlikti visas jam priskirtas funkcijas.
     2. Konsultacijos turi būti teikiamos VLK darbo valandomis, išskyrus atvejus, kai pagalba turi būti teikiama tiek VLK, tiek Išorinio paslaugų teikėjo nedarbo valandomis taip pat švenčių ir poilsio dienomis. Šiuo atveju iš anksto turi būti sudarytas ir suderintas atitinkamų darbų darbo grafikas.
     3. Už AP priežiūros paslaugas su Išoriniu paslaugų teikėju atsiskaitoma kiekvieną mėnesį pagal Išorinio paslaugų teikėjo pasiūlyme nurodytą mėnesinį įkainį.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_