**2.pielikums**

atklāta konkursa nolikumam

“VID informācijas sistēmu savietotāja pilnveidošana, uzturēšana un garantijas nodrošināšana”

iepirkuma identifikācijas Nr. FM VID 2023/197/ĀF

**TEHNISKĀ SPECIFIKĀCIJA**

atklātam konkursam “VID informācijas sistēmu savietotāja pilnveidošana, uzturēšana un garantijas nodrošināšana”, iepirkuma identifikācijas Nr. FM VID 2023/197/ĀF (turpmāk – Konkurss).

Tehniskās specifikācijas sagatavošanas vai pēdējās aktualizācijas datums: 2024.gada 4.janvāris.

Informācija par Konkursa tehniskajām prasībām

SATURS

[1. Ievads 3](#_Toc45724770)

[1.1. Dokumenta nolūks un izmantošana 3](#_Toc45724771)

[1.2. Saīsinājumi un paskaidrojumi 3](#_Toc45724772)

[1.3. Vispārīgs apraksts 5](#_Toc45724773)

[1.4. Saistība ar citiem dokumentiem 7](#_Toc45724774)

[1.5. Dokumenta pārskats 7](#_Toc45724775)

[2. VIDISS esošās situācijas apraksts 8](#_Toc45724776)

[2.1. Loģiskā arhitektūra 8](#_Toc45724777)

[2.1.1. Drošības talonu serviss 10](#_Toc45724778)

[2.1.2. Oracle API Gateway un antivīrusa risinājums 11](#_Toc45724779)

[2.1.3. Oracle Web Tier (iekļauj OHS) 12](#_Toc45724780)

[2.1.4. Oracle SOA Suite (iekļauj WLS, OSB, BPELPM, BAM, MDS, OWSM) 13](#_Toc45724781)

[2.1.5. Oracle Enterprise Repository (OER) 14](#_Toc45724782)

[2.1.6. Lielapjoma datu krātuve (LDK) 15](#_Toc45724783)

[2.1.7. Auditācijas datu krātuve (ADK) 15](#_Toc45724784)

[2.1.8. Drošības zonas 16](#_Toc45724785)

[2.2. Fiziskā arhitektūra 16](#_Toc45724786)

[2.2.1. Komponentu izvietojums pa serveriem 16](#_Toc45724787)

[2.2.2. VIDISS izmantoto datu apraksts 17](#_Toc45724788)

[2.2.3. VIDISS darbināšanai izmantotie serveri 19](#_Toc45724789)

[2.2.4. VIDISS kopējā infrastruktūra 20](#_Toc45724790)

[2.3. VIDISS pārvaldība 21](#_Toc45724791)

[2.3.1. Pārvaldības saskarnes 21](#_Toc45724792)

[2.3.2. Augsta pieejamība un mērogošana 22](#_Toc45724793)

[2.3.3. Uzraudzība (monitorings) 22](#_Toc45724794)

[2.4. VID Web servisu sistēma (VIDWS) 23](#_Toc45724795)

[2.4.1. VIDWS komponentes 23](#_Toc45724796)

[2.4.2. VIDWS resursi 24](#_Toc45724797)

[2.4.3. VIDWS klienti 24](#_Toc45724798)

[2.4.4. VIDWS izpildāmas funkcijas 24](#_Toc45724799)

[2.4.5. VIDWS Web servisi un Web servisu metodes 24](#_Toc45724800)

[2.4.6. VIDWS realizācijas platforma 25](#_Toc45724801)

[3. Prasības Pakalpojumam 26](#_Toc45724802)

[3.1. Prasības Pakalpojuma pārvaldībai 26](#_Toc45724803)

[3.2. Vispārējas prasības Pakalpojumam 28](#_Toc45724804)

[3.3. Prasības pieteikumu apstrādei 28](#_Toc45724805)

[3.4. Prasības nodevumu piegādei un uzstādīšanai 30](#_Toc45724806)

[3.5. Testēšanas prasības 36](#_Toc45724807)

[3.6. Prasības VIDISS pieejamībai un veiktspējai 38](#_Toc45724808)

[3.7. Drošības prasības 38](#_Toc45724809)

[3.8. Prasības Pakalpojuma sniegšanas laikā 42](#_Toc45724810)

# Ievads

## Dokumenta mērķis un izmantošana

Šī dokumenta mērķis ir aprakstīt prasības Valsts ieņēmumu dienesta informācijas sistēmu savietotāja (turpmāk – VIDISS) pilnveidošanas, uzturēšanas un garantijas nodrošināšanas pakalpojumam (turpmāk – Pakalpojums), attiecībā pret kurām tiks veikta Pretendenta iesniegtā piedāvājuma novērtēšana Konkursa ietvaros.

Tehniskā specifikācija ir Pasūtītāja sagatavots un apstiprināts dokuments, kas ir Konkursa dokumentācijas sastāvdaļa. Dokuments ir adresēts Izstrādātājiem, kuri veiks piedāvājumu sagatavošanu, un Pasūtītāja atbildīgajiem darbiniekiem, kuri piedalīsies Konkursa procedūrā.

* 1. Saīsinājumi un paskaidrojumi

1.1. tabula - Saīsinājumi un paskaidrojumi

| **Termins vai saīsinājums** | **Apraksts** |
| --- | --- |
| AAG | Axway API Gateway |
| AD | Active Directory |
| ADCS | Active Directory Certificate Services |
| ADFS | Microsoft Active Directory Federation Service |
| ADK | Auditācijas datu krātuve |
| ARR | Application Request Routing |
| BAM | Oracle Business Activity Monitoring |
| BPELPM | Oracle BPEL Process Manager |
| BR | Oracle Business Rules |
| CSV | Comma-separated values |
| Datubāze | Savstarpēji saistītu datu krājums, ko glabā vienā vai vairākās datnēs |
| DB | Datubāze |
| DNS | Datu noliktavas sistēma |
| DNSWS | DNS ar BusinessObjects Web servisu sistēma |
| DMZ | Demilitarized zone |
| ESS | Oracle Enterprise Scheduler Service |
| FTPS (FTP-SSL) | File Transfer Protocol Secure |
| HTTP | Hyper Text Transport Protocol – Tīkla Internet standartprotokols, kas nodrošina informācijas apmaiņu globālajā tīmeklī. Protokolu HTTP izmanto hipersaišu veidošanai starp hiperteksta dokumentiem. Noklikšķinot peli uz kādas no hipersaitēm, ar šī protokola starpniecību tiek atvērts attiecīgais dokuments neatkarīgi no tā, kur šis dokuments tīklā Internet ir izvietots |
| HTTPS | Secure HyperText Transfer Protocol – Protokola HTTP paplašinājums, kas garantē drošu datu apmaiņu globālajā tīmeklī |
| IIS | Internet Information Services |
| IS | Informācijas sistēma |
| IT | Informācijas tehnoloģija |
| Izstrādātājs | Sākotnēji Konkursa pretendents. Pēc Konkursa iepirkuma līguma tiesību piešķiršanas – līguma izpildītājs. |
| Konkurss | Atklāts konkurss “VID informācijas sistēmu savietotāja pilnveidošana, uzturēšana un garantijas nodrošināšana” |
| LDK | Lielapjoma datu krātuve |
| MDB | mongoDB |
| MDS | Oracle Meta Data Services |
| MED | Oracle Mediator |
| OAG | Oracle API Gateway |
| OER | Oracle Enterprise Repository |
| OSB | Oracle Service Bus |
| OWSM | Oracle Web Services Manager |
| Pakalpojums | Ja nav norādīts citādi, Valsts ieņēmumu dienesta informācijas sistēmu savietotāja pilnveidošanas, uzturēšanas un garantijas nodrošināšana |
| Pasūtītājs vai VID | Valsts ieņēmumu dienests |
| PDF | Portable Document Format |
| PEP | Policy Enforcement Point |
| PPA | Programmatūras projektējuma apraksts |
| PPS | Programmatūras prasību specifikācija |
| SAML | Security Assertion Markup Language |
| SAVI | Sophos Anti Virus Interface |
| SC | Informācijas izmantotājs (Service Consumer) |
| SOA | Service Oriented Architecture |
| SOAP | Simple Object Access Protocol |
| SP | Informācijas avots (Service Provider) |
| SQL | Structured Query Language |
| UDDI | Universal Description, Discovery and Integration – universāls reģistrs – XML formātā internetā veidots reģistrs, kurā apkopota informācija par Web servisu sniedzējiem, servisu veidiem un to operatīvās integrēšanas iespējām |
| UMS | Oracle User Messaging Service |
| VID WS | VID Web servisu sistēma |
| VIDISS | Valsts ieņēmumu dienesta informācijas sistēmu savietotājs |
| VISS | Valsts informācijas sistēmu savietotājs, kas ir ārpus VID IS (nav VIDISS) |
| WAP | Microsoft Web Application Proxy |
| Web servisu metode | Viena no funkcijām, ko nodrošina Web servisi. Paša Web servisa funkcionalitāte tiek veidota no tā Web servisu metodēm |
| WLS | Oracle WebLogic Server |
| WS | Web Services |
| WS-BPEL | Web Services Business Process Execution Language |
| WSDL | Web Services Description Language |
| WT | Oracle Web Tier |
| XML | eXtensible Markup Language |
| XSD | XML Schema Definition Language |

##  Prasību apraksts

Katrai tehniskajā specifikācijā definētai prasībai ir šāda struktūra:

* Indekss – trīsciparu skaitlis, kas tehniskā specifikācijā apzīmē konkrētās prasības kārtas numuru. Indeksu numerācija ir sakārtota augošā secībā sākot ar 001 un ļauj viennozīmīgi identificēt katru konkrēto tehniskajā specifikācijā definēto prasību ar mērķi atvieglot tehniskās specifikācijas lasīšanu un orientēšanos tajā (ātra konkrētās prasības atrašana, tehniskās specifikācijas sasaite ar Konkursa nolikumu u.tml.).
* Prasības nosaukums – ir konkrētas prasības virsraksts, kas sniedz vispārīgu informāciju par prasības saturu.
* Prasības apraksts – ir konkrētās izpildāmās prasības apraksts, kas ir pietiekami detalizēts, lai ļautu Izstrādātājam noteikt prasības realizācijas komplicētību, tādējādi prognozēt nepieciešamo darbietilpību prasības un tehniskās specifikācijas realizācijai kopumā, kā arī Pasūtītājam novērtēt Izstrādātāja tehniskā piedāvājuma atbilstību Konkursa nolikuma mērķiem un uzdevumiem.
* Prasības prioritāte – *Obligāta*(skatīt 1.2.tabulā). Ja prasības formulējumā ir vārds „*vismaz*”, tad prasība nosaka minimālās prasības. Izstrādātājam ir tiesības paplašināt prasības būtību vai ieteikt savādāku veidu, kā nodrošināt to pašu mērķi un vajadzību, piedāvājot, viņaprāt, labāku risinājumu.

1.2. tabula - Prasību prioritātes

|  |  |
| --- | --- |
| Obligāta | Obligāto prasību realizācijas aprakstam jābūt pietiekamam, lai nepārprotami būtu aprakstīts prasības realizācijas mehānisms vai rīki (līdzekļi), ar kuriem ir iespējams realizēt prasību, un Izstrādātāja izpratne par piedāvājamo risinājumu. |

Izstrādātājam piedāvājumā katrai prasībai jāsniedz tās realizācijas (izpildes) apraksts.

Apraksts, kas saturēs prasības teksta kopiju vai tikai prasības izpildes apsolījumu, būs pretrunā ar tehniskās specifikācijas prasībām, kā arī citu prasību realizācijas piedāvājumu, netiks uzskatīts par atbilstošu un šādi piedāvājumi tiks izslēgti no vērtēšanas.

##  Saistība ar normatīvajiem aktiem

Izstrādātājam jānodrošina savu veikto darbu un iesniegto Nodevumu atbilstība ISO/IEC 15408 “Informācijas tehnoloģija – Drošības tehnikas – IT drošības novērtējuma kritēriji” noteiktajām funkcionālajām drošības prasībām, kā arī Izpildītājam jāievēro 02.05.2002. likums “Valsts informācijas sistēmu likums”, Ministru kabineta 2015.gada 28.jūlija noteikumi Nr.442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”, Elektronisko dokumentu likums, Fizisko personu datu apstrādes likums, kā arī VID iekšējie normatīvie akti, kas regulē VID IS drošības nodrošināšanu (VID IS drošības noteikumi, VID Informācijas klasificēšanas un izmantošanas noteikumi, VID IS drošības politika, Personas datu aizsardzības kārtība VID u.c.). Izstrādātājs tiks iepazīstināts ar attiecīgajiem dokumentiem atbilstoši līguma nosacījumiem pēc tā noslēgšanas.

* 1. **Dokumenta pārskats**

Dokuments sastāv no 3 (trim) nodaļām.

Pirmajā nodaļā ir izklāstīts šī dokumenta izstrādāšanas nolūks, aprakstīta darbības sfēra, sniegts dokumenta pārskats, apkopotas izmantotās definīcijas, apzīmējumi un saīsinājumi, dots prasību apraksta skaidrojums un aprakstīta saistība ar normatīvajiem aktiem.

Otrā nodaļa satur VIDISS esošās situācijas aprakstu.

Trešajā nodaļā ir uzskaitītas izvirzītās prasības Pakalpojumam, dots prasību apraksts.

# VIDISS esošās situācijas apraksts

VIDISS ir vienotā augstās pieejamības integrācijas platforma, kas nodrošina VID IS savietojamību neatkarīgi no tehnoloģijām, samazina VID IS savstarpējās atkarības, atvieglo VID IS uzturēšanu un administrēšanu, t.sk. VID IS izmaiņu pārvaldību. VIDISS nodrošina kvalitatīvu un drošu datu apmaiņu starp VID IS, kā arī starp VID IS un citu iestāžu IS, veicinot datu apmaiņu sakārtošanu saskaņā ar mūsdienu prasībām.

VIDISS augstā līmeņa konceptuālās arhitektūras shēmu skat. att.2.1. Uzticamās IS ir gan VID, gan ārējo iestāžu IS, kuras atbalsta federatīvās autentifikācijas pieeju, piemēram, VISS, izmantojot PFAS AUTH. VIDISS integrētās IS (VID IS, ārējo iestāžu IS, uzticamās IS) darbojas gan kā informācijas avots (SP – Service Provider), gan kā informācijas izmantotājs (SC – Service Consumer).

VID pārvaldnieki ir VID darbinieki, kas nodrošina VIDISS un VID IS uzturēšanu.



Att.2.1. VIDISS augstā līmeņa konceptuālās arhitektūras shēma

VIDISS ir izveidots, izmantojot vairāku līmeņu arhitektūru un standartproduktus. VIDISS darbību nodrošina Oracle SOA Suite ietvertie produkti: Oracle API Gateway (centrālais saziņas punkts WS komunikācijai), Oracle Service Bus (WS virtualizācijas slānis), Oracle BPEL Process Manager (servisu apvienošanai vienotā biznesa procesā jeb kompozītā), Oracle Meta Data Services (metadatu repozitorijs) Oracle Enterprise Repository (metadatu pārvaldībai), u.c., kā arī VID prasībām pielāgotie produkti audita un lielapjoma (virs 2 MB) datu uzkrāšanai.

VIDISS kā primārā datubāzes vadības sistēma tiek izmantota Oracle EE 12c, savukārt audita un lielapjoma datu uzkrāšanai – MongoDB.

Lietotāju (t.sk. tehnoloģisko) autentifikāciju un autorizāciju nodrošina Microsoft Active Directory.

Datņu pārbaude pret vīrusiem un ļaundabīgu kodu tiek nodrošināta, izmantojot standartprogrammatūru Sophos Anti Virus Interface.

IS integrācijai tiek izmantoti tīmekļa pakalpojumi (WS). Datu apmaiņu saskarnes tiek nodrošinātas, izmantojot WS-Security specifikācijas paplašinājumu WS-Trust gan VID IS, gan ārējo iestāžu IS. VIDISS nodrošina gan sinhronu, gan asinhrono procesu izpildi. Procesi tiek veidoti kā asinhroni, gadījumos, ja kopējais procesa izpildes laiks pārsniedz 5 sekundes, procesa ietvaros atgriežamais datu apjoms pārsniedz 2 MB, procesa dati ir jāpārbauda pret vīrusiem un/vai ļaundabīgu kodu un/vai procesa izpildē tiek izmantoti vairāk par vienu datu avotu/saņēmēju.

VIDISS nodrošina regulāru fona procesu izpildi, izmantojot standartizētu fona procesu izpildes dzini Oracle Enterprise Scheduler Service.

VIDISS nodrošina integrāciju ar VISS XML katalogu.

## Loģiskā arhitektūra

VIDISS integrēti veido vairāki neatkarīgi servisi, kas kopā veido pilnvērtīgu uz SOA balstītu risinājumu (skat. att.2.2.):

1. Drošības talonu serviss, kas veidots, izmantojot Microsoft Active Directory Federation Service, Microsoft Web Application Proxy, un nodrošina drošības talonu izdošanu SC un federācijas izveidi.
2. Drošības serviss, kas veidots izmantojot Oracle API Gateway un Sophos Anti Virus Interface standartproduktus, un nodrošina VIDISS ārējo saskarni SOAP servisiem, lai tie būtu pieejami SC, kā arī autorizāciju, drošības pārbaudes, darbu ar pielikumiem un pārbaudes pret vīrusiem un/vai ļaundabīgu kodu.
3. Integrācijas serviss, kas veidots, izmantojot Oracle Web Tier un Oracle SOA Suite standartproduktus: Oracle BPEL Process Manager, Oracle Enterprise Scheduler Service, B2B integration, Oracle Mediator un Oracle SOA Suite tehnoloģiskos savienotājus. Šis serviss nodrošina sinhronu, asinhronu procesu izpildi, vairāku SP izmantošanu un procesa stāvokļu saglabāšanu, integrāciju ar dažādu protokolu SP un regulāru fona procesu izpildi.
4. Virtualizēšanas serviss, kas veidots, izmantojot Oracle Web Tier un Oracle SOA Suite standartproduktu Oracle Service Bus, un nodrošina WS virtualizāciju.
5. Metadatu serviss, kas veidots, izmantojot Oracle Meta Data Services un Oracle Enterprise Repository un nodrošina centralizētu metadatu uzglabāšanu (XML shēmas, WSDL definīcijas) un WS dzīves cikla pārvaldību.
6. Datņu serviss, kas veidots, izmantojot lielapjoma datu krātuves risinājumu, un nodrošina datņu glabāšanu VIDISS ietvaros.
7. Auditācijas un monitoringa serviss, kas veidots, izmantojot auditācijas datu krātuves risinājumu, un nodrošina ieejošo un izejošo ziņojumu auditāciju. Lai atbalstītu biznesa monitoringu, izņēmuma gadījumos, kad ziņojumā biznesa dati nav pieejami mašīnlasāmā veidā, tad tiek izmantots Oracle SOA Suite standartprodukts Oracle Business Activity Monitoring.



Att.2.2. VIDISS konceptuālā arhitektūras shēma[[1]](#footnote-2)

Minēto servisu nodrošināšanai tiek izmantota virkne standartproduktu un pielāgoto produktu. Att.2.3. atspoguļotas VIDISS komponentes, kas detalizē att.2.2. minētos servisus.



Att.2.3. VIDISS komponentes

### **Drošības talonu serviss**

DTS nodrošina drošības talonu izsniegšanu VIDISS lietotājiem (t.sk. tehnoloģiskajiem, t.i., VID un ārējo iestāžu IS), izmantojot DTS nodrošināto autentifikācijas metodi. Piemēram, X509 sertifikāts, lietotāja vārds un parole, u.c. Ar izsniegto drošības talonu lietotājs var piekļūt VIDISS WS.

DTS iekļauj šādas komponentes:

* WAP – drošības slānis, kas nodrošina starpniekservera funkcionalitāti, lai paaugstinātu pieejamību un drošību. WAP iekļauj IIS, lai nodrošinātu piekļuvi pie atsaukto sertifikātu saraksta (CRL);
* ADFS – nodrošina autentifikāciju un talonu izdošanu;
* AD – lietotāju datu repozitorijs, kurā tiek glabāti lietotāju dati;
* MS SQL – nodrošina stāvokļa un konfigurācijas informācijas saglabāšanu ADFS augstas pieejamības režīmam;
* ADCS – nodrošina X509 sertifikātu izdošanu, kas nepieciešams IS autentifikācijai un talona izgūšanai no ADFS (scenārijā, ja autentifikācija tiek veikta izmantojot X509). Nodrošina arī ADFS parakstīšanas, šifrēšanas sertifikātu uzturēšanu.



Att.2.4. DTS loģiskā arhitektūra

#### **Autentifikācija**

VIDISS paredz izmantot federatīvās autentifikācijas pieeju, kas tiek atbalstīta ar WS-Security standartiem: pieprasījumatkarīgu autentifikāciju (angl. *claims-based authentication*). Autentifikācijas nodrošināšanai tiek izmantots DTS, kas nodrošina drošības talonu izsniegšanu. Drošības talons satur apliecinājumus par lietotāju, kas vēlas izmantot WS, t.sk. autentifikācijas informāciju (par lietotāja AD lomu/grupu).

#### **Autorizācija**

Autorizācijas funkcionalitāti nodrošina OAG komponents (skat. 2.1.2.app.), balstoties uz DTS autentifikācijas informāciju, kas tiek norādīta talonā ar apliecinājumiem.

VIDISS atsevišķas komponentes nodrošina autentifikācijas un autorizācijas iebūvēto funkcionalitāti administrēšanas vajadzībām. OAG pārbauda saņemto drošības talonu (vai ir uzticams izdevējs) un nodod autorizācijas lēmuma pieņemšanai PEP. PEP talonā sagaida apliecinājumu par subjekta AD lomu/grupu un nodod šo informāciju AA (atribūtu autentifikācijas filtrs). AA pārbauda, vai AD loma/grupa atbilst konkrētā servisa konfigurācijā norādītajai un nodod atbildi PEP. PEP veiksmīgas izpildes gadījumā nodod pieprasījuma izpildi WT, kas tālāk nodod pieprasījuma izpildi SP, savukārt neveiksmīgas izpildes gadījumā OAG sagatavo atbildi izsaucējam par autorizācijas kļūdu.

### **Oracle API Gateway un antivīrusa risinājums**

Oracle API Gateway (OAG) ir jau beidzies produkta uzturēšanas laiks, bet tas vēl tiek lietots, vismaz tik ilgi kamēr netiks veikta visu servisu pārcelšana uz Axway API Gateway (skat.”2.1.3. Axway API Gateway un antivīrusa risinājums”).

OAG ir VIDISS komponente, kas ir integrēta kopā ar SAVI. OAG nodrošina WS publicēšanu gan VID IS, gan IS, kas sadarbojas ar VIDISS no ārējiem VID tīkliem (Internet) un ir centrālais saziņas punkts WS komunikācijai (SOAP, REST, HTTP/S).

OAG nodrošina sākotnējo pieprasījumu apstrādi (drošības talonu autentifikācija, autorizācija, izmantojot drošības talona apliecinājumus, darbs ar pielikumiem, pārbaude pret vīrusiem un ļaundabīgu kodu, SLA mērīšana, WS pieprasījumu izpildes statistikas uzkrāšana, kešatmiņas uzturēšana), pēc kā pieprasījums tiek maršrutēts uz iekšējām VIDISS komponentēm (pēc nepieciešamības WT, OSB, BPELPM, LDK) tālākai izpildei.

OAG ir integrēts kopā ar SAVI un ietver šādas komponentes:

* Policy studio – grafiskā lietotāju saskarne, lai definētu servisu izpildes politikas, kas ietver antivīrusa pārbaudes, WSS, maršrutēšanu pēc satura, šifrēšanu, darbu ar pielikumiem u.t.t.
* Manager – grafiskā lietotāju saskarne procesu pārvaldībai un atsekošanai (tehniskā informācija par OAG instancēm, izsaukumu statistika, procesa definētās politikas pielietošanas izpildes soļu audits, informācija par kļūdām).
* Node manager – rīks, kas nodrošina komunikāciju ar serveru instancēm gan uz atsevišķa servera, gan klasterī.
* Server instance – servera instance, kas praktiski pielieto procesa definētās politikas (OAG servera instances tiek dalītas loģiskās grupās).
* SAVI instance – SAVI instance, kas integrēta ar servera instanci, lai pielietotu antivīrusa pārbaudes saskaņā ar definēto politiku.
* OAG iekšēja kešatmiņas datubāze – nodrošina augstas pieejamības kešatmiņu OAG servera instancēm.

OAG loģiskā arhitektūra ir attēlota att.2.5.



Att.2.5. OAG loģiskā arhitektūra

* + 1. **Axway API Gateway un antivīrusa risinājums**

Axway API Gateway (AAG) ir VIDISS komponente, kas ir integrēts ar atvērtā koda antivīrusa ClamAV. AAG nodrošina WS publicēšanu gan iekšējām IS, gan IS, kas sadarbojas ar VIDISS no ārējiem VID tīkliem (Internet) un ir centrālais saziņas punkts WS komunikācijai (SOAP, REST, HTTP/S). AAG nodrošina virkni filtru (AAG politiku definēšanai), kas paredzēti VIDISS drošības, pārvaldības prasību nodrošināšanai:

* Drošības talonu autentifikācija (atkarībā no talonā izmantotā formāta ir atšķirīgas pārbaudes);
* Autorizācija, izmantojot drošības talona apliecinājumus;
* Darbs ar WS pielikumiem;
* Pārbaude pret vīrusiem un ļaundabīgu kodu;
* SLA (*Service Level Agreement*) mērīšana un informēšana par SLA pārkāpumiem, tai skaitā SNMP ziņojumu izsūtīšanu;
* WS pieprasījumu izpildes statistikas uzkrāšana (tai skaitā statistika par AAG politikā iekļauto darbību izpildi, vai pieprasījuma dati ir jāauditē un kādā apjomā). Piemēram, patērētais laiks veicot pārbaudi pret vīrusiem un ļaundabīgu kodu);
* AAG izpildīto transakciju (AAG servisu izsaukumu) skaita sūtīšana uz Axway Platform;
* Maršrutēšana (arī pēc satura);
* Kešatmiņas uzturēšana, kas nodrošina iespēju WS atbildi saglabāt kešatmiņā un neveikt pieprasījumu uz biznesa servisu ar konfigurējamu iespēju to izmantot/neizmantot/apiet.

AAG nodrošina sākotnējo pieprasījumu apstrādi, pēc kuras pieprasījums tiek maršrutēts gan uz iekšējiem VIDISS komponentiem (pēc nepieciešamības WT, OSB, BPELPM, LDK), gan ārējiem WS (vai nu ārpus VID, vai arī VID IS, kas nav integrētas VIDISS) tālākai izpildei. Lai ārpus VID esošām WS neatklātu VID un VIDISS iekšējā datortīkla uzbūvi, komunikāciju ar ārējām WS ieteicams organizēt tikai izmantojot AAG vai OAG komponentu. Ārējo WS izmantošanas gadījumā, ja tām ir nepieciešama autentifikācija, tad arī to ieteicams realizēt AAG vai OAG komponentā un to izpildīt tieši pirms katras ārējā WS izmantošanas reizes.

AAG ir integrēts kopā ar ClamAV un ietver šādus komponentus:

* Policy studio – grafiskā lietotāju saskarne, lai definētu servisu izpildes politikas, kas ietver antivīrusa pārbaudes, WSS, maršrutēšanu pēc satura, šifrēšanu, darbu ar pielikumiem u.t.t.
* Manager – grafiskā lietotāju saskarne procesu pārvaldībai un atsekošanai (tehniskā informācija par AAG instancēm, izsaukumu statistika, procesa politikas pielietošanas izpildes soļu audits, informācija par kļūdām).
* Node manager – rīks, kas nodrošina komunikāciju ar serveru instancēm gan uz atsevišķa servera, gan klasterī. Tiek izmantots politiku izmaiņu gadījumā.
* Server instance – servera instance, kas praktiski pielieto definētās politikas, kā arī tiešsasitē vai arī manuāli (ar administratora līdzdalību) veic izpildīto transakciju skaita sūtīšana uz Axway Platform. AAG servera instances tiek dalītas loģiskās grupās.
* ClamAV instance – antivīrusa ClamAV instance, kas integrēta ar servera instanci, lai gadījumos, kad politika paredz antivīrusa pārbaudes tās varētu tikt pielietotas.
* AAG iekšēja kešatmiņas datubāze – nodrošina augstas pieejamības kešatmiņu AAG servera instancēm.

Informācija par Axway API Gateway izvietotajiem servisiem tiek apkopota lokāli izvietotā servisu katalogā (Servise Catalog), kuram var piekļūt gan izmantojot Manager rīku, gan arī Axway Portal.

Axway Portal ir rīks ar kuru var gan apskatīties servisu aprakstus, gan arī vieta kur servisu izmantotāji var komunicēt ar servisa izstrādātājiem.

Axway Platform ir Axway mākoņpakalpojums, kurā tiek administrēti mākoņpakalpojuma lietotāji, kā arī tieks uzkrāta informācija par visās VID vidēs izpildīto transakciju skaitu, un var sekot līdz vai tas produkcijas vidē nepārsniedz VID abonēto transakciju skaitu.

AAG loģiskā arhitektūra ir attēlota att.2.6.



Att.2.6. AAG loģiskā arhitektūra

### **Oracle Web Tier (iekļauj OHS)**

WT komponente ir *front-end* serveris OSB un BPELPM un citas komponentes, kas izvietotas uz WLS. WT nodrošina slodzes balansēšanu HTTP pieprasījumiem (t.sk. protokoliem, kas izmanto HTTP, piemēram, SOAP) starp servera instancēm, kas darbojas uz WLS klasterī. WT dekompozīcija ir attēlota att.2.6.

WT iekļauj šādus apakškomponentus:

* OPMN – nodrošina OHS komponenta un apakškomponentu pārvaldību, statistikas vākšanu par OHS procesiem, lai nodrošinātu automātisku procesu pārstartēšanu pie noteiktiem kritērijiem (piem., ilgs atbildes laiks, liela CPU noslodze), identificē komponenta problēmas un nodrošina komandrindas interfeisu;
* OHS – tīmekļa serveris, kas izstrādāts par pamatu izmantojot Apache HTTP tīmekļa serveri, un nodrošina slodzes balansēšanu uz WLS klasteri, izmantojot mod\_wl\_ohs;
* mod\_wl\_ohs –OHS spraudnis, kas paplašina tīmekļa servera funkcionalitāti darbam ar WLS, nodrošinot slodzes dalīšanu uz WLS klasteri;
* WLS managed server –WLS loģiskā servera instance klasterī, uz kura ir izvietoti SOA Suite komponenti (OSB, BPELPM, BAM, OER u.c.).



Att.2.6. WT komponenta loģiskā arhitektūra

### **Oracle SOA Suite (iekļauj WLS, OSB, BPELPM, BAM, MDS, OWSM)**

Oracle SOA Suite ietver virkni komponentu, kas nodrošina VIDISS virtualizēšanas un integrācijas servisus, kā arī infrastruktūras darbināšanai nepieciešamās funkcijas, kas kopā nodrošina SOA infrastruktūru. SOA infrastruktūra nodrošina uz notikumiem balstītu arhitektūru EDA (*Event-Driven Architecture*). EDA tiek izmantota, lai mazinātu savstarpējās saites starp WS – neveicot WS tiešu sasaisti - kontraktu definēšanu, bet balstītu uz notikumiem. Att.2.7. ir attēlota Oracle SOA Suite loģiskā arhitektūra.



Att.2.7. Oracle SOA Suite loģiskā arhitektūra

Oracle SOA Suite iekļautie komponenti nodrošina šādas galvenās funkcijas:

* WLS – lietojumprogrammu serveris, kas nodrošina platformu, uz kuras ir izvietoti Oracle SOA Suite komponenti, līdz ar to nodrošina VIDISS integrācijas un virtualizācijas servisu izpildi. WLS ietver programmatūras infrastruktūras līmeņa servisus, lai atbalstītu lietojumprogrammu un komponentu darbību.
* OSB – nodrošina platformu servisu integrācijai, lai samazinātu divpunktu integrāciju (*point to point integration*) sarežģītību, tādējādi ļaujot veikt izmaiņas IS, samazinot ietekmi uz saistītajām IS. OSB nodrošina standartizētu veidu kā virtualizēt servisus, veikt satura transformāciju un satura bāzētu maršrutēšanu un XSLT atbalstu.
* BPELPM – nodrošina standartizētu veidu, izmantojot BPEL, lai apvienotu atsevišķus servisus vienotā biznesa procesā – saliktā lietojumprogrammā (*composite application*) - kompozītā. BPELPM nodrošina nepieciešamo programmatūras infrastruktūru, lai nodrošinātu šādu kompozītu izpildi (stāvokļu saglabāšanu, ilgu procesu izpildi u.t.t.). BPELPM nodrošina statistikas uzkrāšanu par kompozītu izpildes un pakārtoto procesu izpildes laiku. Kompozītu izpilde var būt automātiska, daļēji automātiska iesaistot cilvēku vai IS, kas pieņem biznesa lēmumu un nodrošina tālāku kompozīta izpildi. Kompozīta biznesa loģika var tikt izpildīta gan secīgi, gan paralēli. BPELPM tiek izmantots dažādu tehnoloģiju apvienošanai vienota biznesa procesa izpildē, kas var iesaistīt gan ārējās IS, gan citus kompozītus, palielinot servisu atkārtotas izmantošanas iespējas.
* MED – nodrošina līdzīgu funkcionalitāti kā OSB. Atšķirība ir MED pielietošanas scenārijos, MED ir izmantojams kā BPELPM komponente, nodrošinot pašā kompozītā starpniecības funkcionalitāti, maršrutēšanu, satura transformāciju, validāciju, ja tāda pēc biznesa loģikas ir nepieciešama.
* BR – izmantojams kā BPELPM komponente, kas nodrošina sarežģītu lēmumu pieņemšanu biznesa procesa izpildē. Strukturēta XML dokumenta apstrāde vai lēmuma pieņemšana balstoties uz datu kopu tiek nodrošināta ar lēmumu tabulām un modificējamajiem likumiem, kas izslēdz nepieciešamību kompozītu izveidē izstrādāt pielāgotas lietojumprogrammas ar “if then” izteiksmēm.
* Oracle JCA Adapters (TS) – tehnoloģiskais savienotājs ir SOA infrastruktūras komponente, kas nodrošina standartizētu pieeju tehniskai integrācijai ar trešajām pusēm neatkarīgi no to izmantojām tehnoloģijām, piegādātājiem un platformām. TS ir būvēti, izmantojot JCA 1.5 atbilstošus resursu adapterus, nodrošinot tehniskus savienojumus ar dažāda veida protokoliem: failu sistēma, FTP, FTPS, *socket*, JMS, AQ, MQ, MS MQ (rindas), UMS, LDAP, datubāzes (jebkura datubāze, kas pieslēdzama ar JDBC draiveri un atbalsta ANSI SQL standartu) un nestandarta protokolu gadījumos ir iespējams pieslēgt un/vai izstrādāt pielāgotus resursa adapterus, kas atbalsta JCA 1.5.
* MDS – tiek izmantots failu bāzēts metadatu (XML shēmas, WSDL definīcijas) repozitorijs gan OSB, gan BPELPM kompozītiem. Lai nodrošinātu centralizētu metadatu uzturēšanu un ilgtermiņā atvieglotu izstrādi, pārvaldību, tiek izmantots DB MDS. MDS nodrošina jau gatavas DB shēmas šādu vajadzību nodrošināšanai SOA infrastruktūras līmenī.
* OWSM – nodrošina drošības infrastruktūru un drošības politikas WS atbilstoši WSS prasībām. OWSM nodrošina šādas drošības prasības kā autentifikāciju, autorizāciju, konfidencialitāti un privātumu, integritāti un nodrošina pasākumus pret dalības noliegumu (*non-repudiation*).
* BAM – nodrošina reāllaika biznesa datu auditāciju un analīzi (KPI biznesa mērījumus). BAM izmantošana ir ieslēdzama BPELPM kompozītiem.
* ESS – procesu izpildes plānotājs, kas nodrošina regulāru procesu izpildi SOA infrastruktūras līmenī. ESS ir izmantojams scenārijos, kad ir nepieciešams automātiski izpildīt kādu biznesa procesu. ESS ļauj ieplānot un pārvaldīt procesu izpildes grafikus.
* UMS – infrastruktūras līmeņa serviss, kas nodrošina ieejošās/izejošās saziņas nodrošināšanu ar gala lietotājiem, izmatojot kādu no standarta kanāliem: e-pasts, SMS vai tūlītējās ziņojumapmaiņas (*instant messaging*) servisiem. Ienākošie ziņojumi var tikt apstrādāti automātiski un iedarbināt dažādus apstrādes procesus.

### **Oracle Enterprise Repository (OER)**

OER nodrošina servisu un XML shēmu katalogu, kas realizē centralizētu servisu pārvaldību un šo servisu publicēšanu, nodrošinot servisu dzīves cikla pārvaldību, kā arī uz standartiem bāzētu sadarbību ar SOA platformas komponentiem (OSB, BPEL) un palīdz nodrošināt servisu atkārtotu izmantošanu. OER komponente darbojas uz WLS un tā darbināšanai ir nepieciešama DB, kur tiek apkopota informācija par servisu metadatiem no OAG, OSB, BPELPM komponentēm un ārējām IS.



Att.2.8. OER loģiskā arhitektūra

OER nodrošina tādu resursu metadatu uzglabāšanu kā XML shēmas un servisu WSDL definīcijas. XSD resursi tiek sadalīti trīs grupās:

(1) IVIS XSD

- balstās uz VISS XML shēmu izstrādes vadlīniju standarta,

- primāra XML shēmu glabātuve ir VISS XML resursu katalogs,

- tiek importēti un aktualizēti OER ar automatizētas procedūras palīdzību.

(2) VID XSD

- balstās uz VID XML shēmu izstrādes vadlīniju standarta, kas savukārt balstās uz VISS XML shēmu izstrādes vadlīniju standarta,

- primāra XML shēmu glabātuve ir VID OER.

(3) Eiropas vai citas XML shēmas

- primāra XML shēmu glabātuve ir VID OER.

### **Lielapjoma datu krātuve (LDK)**

LDK nodrošina ienākošo strukturēto un nestrukturēto ziņojumu (virs 2 MB) pielikumu glabātuvi/servisu. LDK mērķis ir samazināt datņu pārsūtīšanu starp procesa soļiem vai IS, nodalot datnes no paša ziņojuma.

LDK nodrošina datnes kontrolsummas uzturēšanu, kontrolsumma tiek parakstīta ar LDK risinājuma sertifikātu (tehnisko procesu), kas apliecina kontrolsummas autentiskumu un garantē, ka atbilstošais LDK uzglabājamais objekts nav modificēts.

LDK veido šādas komponentes:

* LDK datubāze – NoSQL datubāze, kur par pamatu tiek izmantota MongoDB un kas nodrošina horizontālas un vertikālas mērogošanas iespējas.
* CMIS 1.1 SOAP saskarne – funkciju kopums, kas nodrošina pamatdarbības ar dokumentiem (pievienošanu, aktualizāciju, meklēšanu, kategorizēšanu utt.) uz CMIS 1.1 standarta bāzes.
* LDK lietotāju saskarne – administrēšanas konsole LDK pārvaldībai, kas nodrošina dokumentu konfigurāciju, meklēšanu, pievienošanu, kopēšanu utt.

OAG/OSB/BPELPM izmanto LDK strukturēto un nestrukturēto dokumentu pagaidu vai pastāvīgai uzglabāšanai, izmantojot savstarpējā apmaiņā atsauces – dokumentu (vai dokumentu mapes) unikālos identifikatorus.

### **Auditācijas datu krātuve (ADK)**

ADK nodrošina ienākošo un izejošo ziņojumu auditu. ADK veido šādas komponentes:

* ADK datubāze - NoSQL datubāze, kur par pamatu tiek izmantota MongoDB un kas nodrošina horizontālās un vertikālās mērogošanas iespējas. Pirms auditācijas ierakstu dzēšanas tiek nodrošināta auditācijas pierakstu automātiska pārnešana uz šim nolūkam izveidotu MongoDB arhīva datubāzi.
* Auditācijas ierakstu uzkrāšanas WS – asinhrons iekšējais WS, kas nodrošina auditācijas ierakstu pieņemšanu no OSB eksponētiem servisiem, LDK u.t.t. Ņemot vērā to, ka auditācijas ierakstu validācija un saglabāšana ir asinhrons process, kļūdas tiek fiksētas sistēmas žurnālā un netiek paziņotas mērķa IS.
* ADK lietotāju saskarne – administrēšanas konsole ADK pārvaldībai (uzkrāto auditācijas ierakstu meklēšanai un apskatei).

### **Drošības zonas**

VIDISS aizsardzībai no arējiem riska faktoriem VIDISS ir sadalīts drošības zonās, kur katrai drošības zonai tiek uzstādītas savas drošības prasības. Nodaļā ir aprakstīts VIDISS sadalījums drošības zonās un katras zonas drošības ierobežojumi:

* Ārējā zona – zona, kas ietver Internet un citus tīklus, kas nav VID pārziņā uz ko nevar attiecināt drošības ierobežojumus.
* VID zona – šajā zonā atrodas VID IS un lietotāji. Šajā zonā atrodas resursi, kas ir ārpus VIDISS, uz kuriem neattiecas VIDISS drošības prasības.
* Aizsargājamā zona – šajā zonā izvietotas komponentes komunikācijai ar IS, izmantojot WS. IS var atrasties gan VID, gan ārējā zonā. Šī ir VIDISS zona, kas nodrošina VIDISS aizsardzību no resursiem, kas nav VIDISS sastāvdaļa. Šī zona uzskatāma par DMZ (tiek izmantoti komunikācijas portu ierobežojumi, komunikācijas kanāla šifrēšana). Šīs zonas komunikācijā tiek veikta informācijas (XML ziņojuma) parakstīšana un paraksta pārbaude, lai nodrošinātu šī ziņojuma aizsardzību pret modificēšanu ziņojuma pārraides laikā.
* Uzticamā zona – šajā zonā VIDISS komponentes sadarbojas uzticamas apakšsistēmas režīmā. No šīs zonas virtualizācijas serviss var komunicēt ar VID zonas VID IS WS, kas nodrošina WSS. Integrācijas serviss var komunicēt ar VID zonas vai arī ārējās zonas IS, kas nenodrošina WS interfeisus. Ja IS atrodas ārējā zonā, tad šādā gadījumā jāveido drošs tīkla savienojums.

## Fiziskā arhitektūra

Šī nodaļa apraksta VIDISS izvietojumu VID infrastruktūrā.

## 2.2.1. Komponenšu izvietojums pa serveriem

Šajā nodaļā ir aprakstīts VIDISS komponenšu izvietojums serveros (klastera serveru grupās). Šī atbilstība ir attēlota 2.1. tab. Norādītais servera grupas nosaukums ir izmantots norādot konkrētu servera nosaukumu.

2.1. tabula Komponentu izvietojums pa serveriem

| **Servera grupas nosaukums** | **Izvietojamās komponentes** |
| --- | --- |
| ADCS | ADCS |
| ADFS | ADFS |
| LDK | LDK lietojumprogramma |
| WAP | WAP |
| ARR | ARR |
| ADK | ADK lietojumprogramma |
| MDB | MongoDB: ADK un LDK DB |
| OAG | OAG, SAVI |
| AGW | AAG, ClamAV |
| OER | WLS, OER |
| BPELPM | WLS, OWSM, MDS, BPELPM, MED, BR, TS, BAM, ESS, UMS |
| WT | WT |
| OSB | WLS, OWSM, MDS, OSB |

## 2.2.2. VIDISS izmantoto datu apraksts

Šajā nodaļā aprakstīta komponenšu nozīme datu apstrādē un datu apmaiņu izstrādes procesā.

2.2. tabula VIDISS komponenšu iesaiste datu apstrādē un izstrādes procesā

| **Servera grupas nosaukums** | **Apstrādājamie dati** | **Iesaiste datu apmaiņu izstrādē** |
| --- | --- | --- |
| ADCS | Autentifikācijas informācija. SSL un X509 sertifikāti. | Nav. |
| ADFS | Autentifikācijas informācija. Apstrādā X509 sertifikātus, lietotāju vārdus, paroles, drošības talonus. Nodrošina saiti ar AD. | Pie drošības talona satura izmaiņām un jaunu aizsargātu WS reģistrācijas ir jāveic konfigurācijas izmaiņas. |
| LDK | Apstrādā biznesa datus - WS pielikumus (dažāda formāta), asinhronas atbildes, liela apjoma XML dokumentus. | Nav.  |
| WAP | Nodrošina slodzes balansēšanu DTS apakškomponentiem. Datu apstrāde netiek veikta. | Nav. |
| ARR | Nodrošina slodzes balansēšanu LDK, ADK apakškomponentiem. Datu apstrāde netiek veikta. | Nav. |
| ADK | Apstrādā biznesa datus - WS pieprasījumus/atbildes. | Nav.  |
| MDB | Uzkrāj datus, kas tiek pārsūtīti VIDISS (audita informācija – XML pieprasījumi/atbildes un VIDISS pārsūtītās datnes/ WS pielikumi). | Nav. |
| OAG | Atstrādā autentifikācijas informāciju - drošības talonus, to saturu. Apstrādā trešās puses autentifikācijas informāciju (lietotāja vārds/ parole, X509 sertifikāti). Apstrādā biznesa datus - WS pieprasījumus/atbildes (tai skaitā WS pielikumus). Uzkrāj OAG politiku aprakstus. | Ir jāveic OAG politiku izstrāde un piegāde ar datu apmaiņām, ja datu apmaiņas neiekļaujas jau OAG esošās politikās. |
| AGW | Apstrādā autentifikācijas informāciju - drošības talonus, to saturu. Apstrādā trešās puses autentifikācijas informāciju (lietotāja vārds/ parole, X509 sertifikāti). Apstrādā biznesa datus WS pieprasījumi/atbildes (tai skaitā WS pielikumus). Uzkrāj AAG politiku aprakstus. | Ir jāveic AAG politiku izstrāde un piegāde ar datu apmaiņām, ja datu apmaiņas neiekļaujas jau AAG esošās politikās. |
| OER | Apkopo informāciju par VIDISS izmantotajiem WS (XML shēmas, WSDL definīcijas). | Pie jaunu WS izveides ir jāreģistrē metadati, lai atvieglotu WS pārvaldību. |
| BPELPM | Atstrādā autentifikācijas informāciju - drošības talonus, to saturu. Apstrādā biznesa datus- WS pieprasījumus/atbildes. Uzkrāj AD informāciju par kontiem un grupām (automātiska sinhronizācija autorizācijas vajadzībām).Uzkrāj kompozītu aprakstus. | Jāveic datu apmaiņas kompozīta izveide un piegāde. |
| WT | Nodrošina slodzes balansēšanu OSB un BPELPM. Datu apstrāde netiek veikta. | Nav. |
| OSB | Apstrādā autentifikācijas informāciju - drošības talonus, to saturu. Apstrādā biznesa datus - WS pieprasījumus/atbildes. Uzkrāj AD informāciju par kontiem un grupām (automātiska sinhronizācija autorizācijas vajadzībām).Uzkrāj kompozītu aprakstus. | Jāveic datu apmaiņas kompozīta izveide un piegāde. |

## VIDISS darbināšanai izmantotie serveri

Šajā nodaļā ir aprakstīti VIDISS darbināšanai izmantotie serveri. VIDISS izmitināts lietojumprogrammatūra uz x86 arhitektūras serveriem ar Linux operētājsistēmu, izmantojot Citrix XenServer virtualizāciju, savukārt datubāze ir izvietota uz lieljaudas servera Oracle SuperCluster ar Sparc procesoriem un Solaris operētājsistēmu, virtuālizācijai izmantojot Solaris zonas.

VIDISS vienas vides (produkcijas) darbināšanai tiek izmantoti virtuālie serveri, kas aprakstīti 2.3. tabulā. Testa vides darbināšanai ir izdalīts vēl viens šāds virtuālo serveru komplekts (testa serveri šajā dokumentā attēloti ar prefiksu “T” servera nosaukumā).

VIDISS tiek darbināts viena datu centra ietvaros, bet VIDISS arhitektūra paredz VIDISS darbināšanu divos datu centros. VIDISS vienas vides darbināšanai tiek izmantotas šādas VID sistēmas, kas aprakstītas 2.3. tabulā.

2.3. tabula VIDISS darbināšanai nepieciešamās VID sistēmas

|  |  |
| --- | --- |
| **Nosaukums**  | **Apraksts** |
| ADCS-A1 | AD certificate services (vismaz MS Windows Server 2008) |
| SQL-A1  | MS SQL Server 2012 R2 |
| AD-A1  | AD (MS Windows Server 2012) |
| Oracle-A1  | Oracle RAC DB (Oracle DBVS 12c). Šis serveris tiks izmantots VIDISS DB shēmu izveidei un datu glabāšanai. |

## 2.2.4. VIDISS kopējā infrastruktūra

VIDISS testa un produkcijas vides ir nodalītas visu komponenšu tvērumā. VIDISS izvietojumā ir attēloti serveri (un atbilstošās komponentes, kas izvietotas uz šī servera) un augstas pieejamības mehānismi, kas nodrošina VIDISS bojājumpacietību:

* cluster – paredz izmantot vienu aktīvu servera instanci katrā datu centrā. Datu centra ietvaros klastera koordinators nodrošina pārslēgšanos starp servera instancēm, nodrošinot slodzes dalīšanu. Servera instances kļūdas gadījumā tā tiek izslēgta no klastera, līdz tā atkal spēj apstrādāt pieprasījumus. Datu uzglabāšanas gadījumā, kad netiek izmantota Oracle RAC DB (komponente MDB) tiek veikta datu replikācija (*replication*) starp serveru instancēm.
* active-active – paredz izmantot vairākas aktīvas servera instances (klasteris)., kur klasteris apstrādā pieprasījumus no NLB (*active-active* režīmā). NLB nodrošina slodzes balansēšanu uz servera instancēm un uzrauga vai servera instance ir pieejama.
* Data Guard – ir iespējams izmantot esošo risinājumu – *Oracle Real Application Clusters* (Oracle DB papildu programmatūra, kas nodrošina DB klasteru izveidi un augstu pieejamības nodrošināšanu).
* AlwaysOn Availability Groups – ir Microsoft SQL Server papildu programmatūra, kas nodrošina DB augstu pieejamību.
* standalone – paredz, ka tiek darbinātas vairākas neatkarīgas serveru instances, kas nav iekļautas vienotā klasterī, taču darbojas active-active režīmā. NLB nodrošina slodzes balansēšanu uz šīm servera instancēm un uzrauga vai šī servera instance ir pieejama.

Šāds VIDISS izvietojums nodrošina VIDISS komponenšu mērogojamību, pievienojot jaunus fiziskos vai virtuālos serverus, bez papildus programmēšanas darbiem. Pievienojot jaunu serveri (fizisko, virtuālo), uz kura ir izvietota kāda no VIDISS komponentēm ir jāveic atbilstošās komponentes klastera pārkonfigurēšana.

Datu apmaiņas kompozīti un VIDISS tehniskie servisi tiks izvietoti klasterī uz vairākiem serveriem, lai nodrošinātu ne tikai VIDISS infrastruktūras, bet arī pašu datu apmaiņu augstu pieejamību. Ar VIDISS serveru izvietojuma shēmu pretendents var iepazīties klātienē VID telpās.

Ir izdalīts atsevišķs pārvaldības tīkls, lai administratoriem nodrošinātu piekļuvi pie visiem VIDISS serveriem.

## VIDISS pārvaldība

### **Pārvaldības saskarnes**

VIDISS uzturēšanai tiek izmantotas komponenšu pārvaldības saskarnes (grafiskās lietotāja saskarnes):

2.4. tabula Galvenās VIDISS pārvaldības saskarnes

| **Nosaukums** | **Apraksts** |
| --- | --- |
| /console | Tīmekļa lietojumprogramma, kas nodrošina WLS administrēšanas iespējas (konfigurācijas parametru izmaiņas, *managed server* startēšana/apturēšana, diagnostika, datu avotu pārvaldība u.t.t.). |
| /em | Tīmekļa lietojumprogramma, kas nodrošina komponenšu, kas izvietotas uz WLS (BPELPM, OSB, OWSM u.c.) pārvaldību (konfigurācijas izmaiņu veikšanu, WSS konfigurēšanu). Nodrošina detalizētu kompozītu (biznesa procesa, darba plūsmas) izpildes soļu apskati (BPEL procesiem) un arī OHS pārvaldību, ja uz WLS ir uzstādīts OHS. Nodrošina kompozītu izsaukšanu testēšanas vajadzībām. |
| /bam/composer | Tīmekļa lietojumprogramma, kas nodrošina piekļuvi BAM pārskatiem un nodrošina dinamisku pārskatu sagatavošanu tiešsaistē. |
| /servicebus | Tīmekļa lietojumprogramma, kas nodrošina OSB kompozītu pārvaldību. |
| ADFS pārvaldības konsole | Lietojumprogramma, lai administrētu DTS talonu izdošanu (talonu saturu, sertifikātus un WS kuriem tiks izdoti taloni, u.c. funkcijas). |
| OAG un AAG policy studio | Grafiskā lietotāju saskarne, lai definētu servisu izpildes politikas, kas ietver antivīrusa pārbaudes, WSS, maršrutēšanu pēc satura, šifrēšanu, darbu ar pielikumiem u.t.t. |
| OAG manager | Tīmekļa lietojumprogramma, lai uzraudzītu OAG darbību – iegūtu statistiku par izsaukumiem un to izpildi (veiksmīgi, neveiksmīgi, kļūdu apraksti, u.t.t.). |
| AAG manager | Tīmekļa lietojumprogramma, lai uzraudzītu AAG darbību – iegūtu statistiku par izsaukumiem un to izpildi (veiksmīgi, neveiksmīgi, kļūdu apraksti, u.t.t.). |
| AAG Portal | Tīmekļa lietojumprogramma, lai apskatītu AAG servisu katalogā esošo informāciju un nodrošinātu iespēju servisu izmantotājiem komunicēt ar servisu izstrādātājiem |
| Axway Platform | Tīmekļa mākoņpakalpojuma lietojumprogramma kurā var administrēt VID kontu Axway produktu izmantošanai un sekot līdz cik daudz Gateway transakciju jau ir izlietots |
| WLST | WebLogic Scripting Tool (WLST) nodrošina komandrindas interfeisu, lai administrētu Risinājuma komponentes, kas izvietotas uz WLS. |
| /soa/composer/ | Tīmekļa lietojumprogramma, kas nodrošina piekļuvi BPEL definētajiem procesiem, pārvaldību un nodrošina izmaiņu veikšanu BPEL procesiem saskaņā ar WS-BPEL. Nodrošina iespējas arī veikt izmaiņas BR. |
| JDeveloper | Izstrādes rīks, kas nodrošina jaunu BPEL procesu izveidi – kompozītu izstrādi saskaņā ar WS-BPEL. |

### **Augsta pieejamība un mērogošana**

VIDISS ir mērogojams gan viena datu centra ietvaros, gan divos datu centros. Augstas pieejamības nodrošināšanai tiek izmantoti datubāzes klasteri un tīkla slodzes dalīšanas risinājumi, Citrix netscaler un Oracle Web Tier. IZPILDĪTĀJS var iepazīties ar VIDISS kopējās infrastruktūras, datortīkla infrastruktūras aprakstu klātienē VID telpās.

### **Uzraudzība (monitorings)**

Serveru uzraudzībai (diski, procesori, atmiņa, žurnālfaili) tiek izmantots VID rīcībā esošais IS uzraudzības rīks Zabbix (turpmāk Zabbix). Zabbix tiek izmantots, lai pārvaldītu arī kritiskos servisus: DTS, datņu izmantošanas WS, auditācijas WS. Šo servisu uzraudzības pieeja ir līdzvērtīga kā aprakstīts 6.4 nodaļā, izmantojot darbspējas pārbaudi (health check).

OAG paredz izmantot SNMP brīdinājumu izsūtīšanu uz Zabbix, ja datu apmaiņas izpildē ir radušās tehniskas kļūdas vai pārkāpts datu apmaiņas SLA.

## VID Web servisu sistēma (VIDWS)

VID Web servisu sistēma (VIDWS) kā VIDISS komponente paredzēta, lai nodrošinātu Pasūtītāja informācijas apmaiņu ar dažādām ārējām IS, kā arī Pasūtītāja informācijas sistēmu starpā.

* + 1. VIDWS komponentes
* **Web servisi** ir centrālā komponente visā VIDWS. Web servisi sastāv no vairākām metodēm, un katra realizē savu prasību. Web servisi darbojas lietojumu serverī. Lietojumu serverim jānodrošina Web servera darbība, t.i., tam jāatbalsta protokoli WSDL, SOAP un HTTPS. Web servisi savā darbībā griežas pie lokālās datu bāzes VIDWS DB.
* **VIDWS DB** paredzēta šādu VIDWS Web servisu specifisko datu glabāšanai
	+ kļūdu žurnāls;
	+ Web servisu metožu izsaukumu žurnāls;
	+ lietotāju saraksts kopā ar lietotāju tiesībām un kvotām;
	+ profili;
	+ lietotāju grupu saraksts;
	+ pārskatu saraksts un to parametri;
	+ Web servisu metožu klasifikators;
	+ lietotāju pieprasījumi.
* **Pieprasījumu pārbaudes process** paredzēts DNSWS regulārai aptaujai ar mērķi noskaidrot, vai lietotāja prasītais pārskats ir gatavs, vai nē. Ja pārskats ir gatavs, tad tas tiek fiksēts VIDWS DB. VIDWS DB tiek arī saglabāts pats gatavais pārskats visos vajadzīgajos formātos. Šāds process ir nepieciešams tikai asinhronu izsaukumu gadījumā.
* **Atgriezeniskās saites nodrošināšanas process** nosūta klientam paziņojumu par pieprasījuma izpildi tiem klientiem, kuri ir pieprasījuši tādu paziņojumu. Pēc šī paziņojuma saņemšanas klients no VIDWS var savākt prasīto pārskatu. Atgriezeniskās saites funkcijai ir variants, kad klientam kopā ar paziņojumu par pieprasījuma beigām tiek aizsūtīts pats pārskats. Atgriezeniskās saites nodrošināšanas process strādā fonā un regulāri griežas pie VIDWS DB un nosaka, kuri pieprasījumi ir apstrādāti, aizsūta pabeigto pieprasījumu lietotājiem paziņojumus (kopā ar pašu pārskatu, ja tas ir bijis prasīts) par pieprasījumu izpildes beigām. Šāds process ir nepieciešams tikai asinhronu izsaukumu gadījumā.
* **Administrēšanas programma** ir vajadzīga, lai administrētu VIDWS, t.i., mainītu tās parametrus, veidotu jaunas lietotāju grupas, reģistrētu jaunus lietotājus, piešķirtu lietotājiem tiesības, sekotu VIDWS darbībai utt.

## VIDWS resursi

VIDWS resursi ir informācijas sistēmas, datubāzes un faili, pie kuriem VIDWS var griezties, lai atbildētu uz klienta pieprasījumiem (sk.1.1.zīm.). Ar katru no šiem resursiem VIDWS var komunicēt atšķirīgi un tas ir atkarīgs no paša resursa. DNSWS ir Web servisi, kuri nodrošina saskarni ar DNS. Resursu sistēmu datubāzēm tiek izmantotas Sybase IQ, Oracle, IBM Netezza un IBM Informix tehnoloģijas. Resursu sistēmu datubāzēs tiek veidotas un izmantotas arī datu atlases procedūras VIDWS vajadzībām.

## VIDWS klienti

VIDWS klienti ir Pasūtītāja iekšējās IS un ārējo organizāciju IS. Klienti komunicē ar VIDWS ar SOAP protokola starpniecību.

Tīkls savieno VIDWS ar klientiem. Lokālais tīkls ir drošs tīkls, kurā var nelietot drošības protokolu HTTPS un serveru līmenī fiksēt komunikācijā iesaistīto serveru adreses. Ja klients pieslēdzas VIDWS, izmantojot Interneta tīklu, tad HTTPS protokola izmantošana ir obligāta.

## VIDWS izpildāmas funkcijas

VIDWS nodrošina saskarni ar Pasūtītāja iekšējām IS un ārējo organizāciju IS (VIDWS klienti). VIDWS klienti pieslēdzas Web servisam un noteiktā secībā izsauc vajadzīgās metodes. VIDWS Web servisu aprakstu klients var dabūt no publicētā WSDL faila, kurā ir visa nepieciešamā informācija jebkuras VIDWS metodes izsaukšanai.

## VIDWS Web servisi un Web servisu metodes

VIDWS Web servisi ir Web servisi, ar kuru metožu palīdzību notiek datu apmaiņa starp dažādām Pasūtītāja IS un starp Pasūtītāja IS un ārējo organizāciju IS.

VIDWS Web servisus kopīgs karkass, kura ietvaros implementēta katra Web servisu metode, nodrošina šādas kopējas funkcijas:

* lietotāju autorizāciju;
* lietotāju pieejas kontroli dažādām Web servisu metodēm un pārskatiem;
* Web servisu metožu izpildes biežuma kontroli, lai novērstu ļaunprātīgu Web servisa izmantošanu;
* nodrošina pieeju dažādiem resursiem, tādiem kā DB un faili, kā arī nodrošina darbu ar šiem resursiem (parasti šīs funkcijas nodrošina programmatūras izstrādes vides un lietojumu serveris);
* Web servisu metožu izsaukumu protokolēšanu;
* vienotu kļūdu apstrādes un ziņošanas mehānismu;
* Web servisu funkcionēšanu, t.i., SOAP ziņojumu sūtīšanu un saņemšanu, WSDL faila izveidi u.t.t. (parasti šīs funkcijas nodrošina programmatūras izstrādes vides un lietojumu serveris).

VIDWS Web servisu metodes iedalāmas divās grupās: sinhronās un asinhronās. VID Web servisi satur autorizācijas metodes (sinhronas) un informācijas iegūšanas metodes (gan sinhronas, gan asinhronas). VIDWS Web servisu metodes izpildās pēc pieprasījuma un/vai atbilstoši sistēmas parametra vērtībai.

## VIDWS realizācijas platforma

* Web servisu nodrošinājums: SOAP versija 1.1 un WSDL versija 1.1 vai jaunāka.
* Lietojumserveris: Oracle WebLogic Application Server 12c vai jaunāks.
* VIDWS DB: Oracle 12c vai jaunāka.
* Programmēšanas valoda: Java 2.
* Web servisu implementācijas modelis: JAX-RPC v1.1.

# Prasības Pakalpojumam

## Prasības Pakalpojuma pārvaldībai

1. **Pakalpojuma uzturēšanas un pilnveidošanas darbu uzsākšana (Obligāta)**

 Pēc līguma noslēgšanas Pasūtītājs 5 (piecu) darba dienu laikā nodod Izpildītājam Sistēmas pirmkodus, izpildkodus un pilnu tehnisko dokumentāciju, kas ir viņa rīcībā, kā arī informāciju par VID rīcībā esošo un Sistēmas darbināšanā izmantoto standartprogrammatūru un tās aktuālajām versijām. Izpildītājam 20 (divdesmit) darba dienu laikā no šajā punktā minētās informācijas saņemšanas jāuzsāk Sistēmas uzturēšana.

Sākot ar 21.dienu, Sistēmas uzturēšana jānodrošina šādās fāzēs atbilstoši problēmu klasifikācijai (0.1.0.pielikuma 2.3. apakšpunkts Līgumā):

|  |  |
| --- | --- |
| **Svarīgums VID ISIPS** | **Reakcijas laiks no RZ saņemšanas brīža** |
|  | **Pārejas posmā**  | **Pamatdarbības posmā**  |
| Kritisks | Ne lielāks par 4 (četrām) VID darba stundām (VID darba laiks noteikts šī pielikuma 7.2.apakšpunktā) |
| Steidzams | Ne lielāks par 10 (desmit) VID darba stundām. | Ne lielāks par 8 (astoņām) VID darba stundām |
| Parasts | Ne lielāks par 28 (divdesmit astoņām) VID darba stundām. | Ne lielāks par 24 (divdesmit četrām) VID darba stundām |

Pārejas posmā VID nodrošinās atbalstu Sistēmas pirmkoda, izpildkodu un tehniskās dokumentācijas pārņemšanā.

1. **Izstrādes, testa vides nodrošināšana (Obligāta)**

Izstrādātājam ir jānodrošina sava izstrādes un testēšanas vide (aparatūra, programmatūra, biroja telpas) līguma ietvaros izpildāmo darbu un uzdevumu veikšanai.

Pasūtītājs nodrošina ar sistēmu izstrādei nepieciešamajām datu kopu struktūrām un informāciju, kas nepieciešama pieslēgumu simulācijai ārējām sistēmām, bet nenodrošina fiziskus pieslēgumus Pasūtītāja testa vidēm.

Izstrādātājam izstrāde un testēšana jāveic, izmantojot tikai licencētu vai bezmaksas programmatūru. Pasūtītājs nenodrošina Izstrādātāju ar programmatūras licencēm. Izstrādātājs nedrīkst izmantot programmēšanas rīkus vai līdzekļus, kas prasītu papildu licenču iegādi Pasūtītājam.

1. **Pakalpojumā izmantojamā valoda (Obligāta)**

Izstrādātājam visā Pakalpojuma sniegšanas laikā visi Nodevumi jānoformē latviešu valodā un komunikācija ar Pasūtītāju jānodrošina tikai latviešu valodā. Ja tiks piesaistīti speciālisti, kuri nepārvalda latviešu valodu, Izstrādātājam šo speciālistu saziņā ar Pasūtītāju jānodrošina tulkošana bez papildu maksas. Rakstiskajā komunikācijā nav pieļaujama tikai automātisko tulkošanas rīku (piemēram: *Google Translate*) izmantošana.

1. **Pakalpojuma bibliotēka (Obligāta)**

Izstrādātājam Pakalpojuma sniegšanas laikā ir jāuztur Pakalpojuma bibliotēka atbilstoši Līguma 4.42. un 4.43.apakšpunktā noteiktajam. Pakalpojuma bibliotēkā jāizvieto un jāuztur visi Pakalpojuma dokumenti – prasību specifikācijas, projektējuma apraksti, testēšanas dokumentācija u.c. Izstrādātājam pēc VID pieprasījuma jānodrošina VID piekļuve Pakalpojuma bibliotēkai.

1. **Pakalpojuma problēmu vadība (Obligāta)**

Izstrādātājam ir jāidentificē Pakalpojuma problēmas un savlaicīgi jāziņo par tām Pasūtītājam, kopīgi ar Pasūtītāju nosakot nepieciešamās korektīvās darbības un kontrolējot to izpildes efektivitāti.

1. **Pakalpojuma risku vadība (Obligāta)**

Izstrādātājam visā Pakalpojuma sniegšanas laikā ir jāveic ar Pakalpojuma sniegšanu saistīto risku identificēšana, analīze, novērtēšana, uzraudzība un kontrole, risku mazināšanas un/vai novēršanas darbu plānošana un īstenošana.

Izstrādātājam tehniskajā piedāvājumā ir jāapraksta ar Pakalpojuma sniegšanu saistīto sākotnējo risku novērtējums, kā arī pieņēmumi, atkarības un ārējās ietekmes, kas tika ņemtas vērā, sagatavojot piedāvājumu.

Izstrādātājam tehniskajā piedāvājumā ir jāapraksta risku vadības pieeja, ko Izstrādātājs izmantos ar Pakalpojuma sniegšanu saistīto risku vadībai.

1. **Plānu pārvaldība**

Izstrādātājam Pakalpojuma sniegšanas laikā jānodrošina Pakalpojuma sniegšanai nepieciešamo plānu pārvaldība saskaņā ar Līguma 0.2.0.pielikuma 1.1.apakšpunktu.

1. **Speciālistu savstarpējās sadarbības un komunikācijas shēma** **(Obligāta)**

Izstrādātājam jānodrošina efektīva Izstrādātāja speciālistu komunikācija ar Pasūtītāja speciālistiem. Nepieciešamības gadījumā nodrošināt attālinātās sanāksmes, izmantojot, piemēram, Microsoft Teams, Zoom.

Izstrādātājam jāiesniedz shēma, kurā attēlota Izstrādātāja speciālistu komunikācija ar Pasūtītāja speciālistiem.

1. **Kvalitātes vadība** **(Obligāta)**

Izstrādātājam Pakalpojuma sniegšanas laikā ir jānodrošina kvalitātes pārvaldības procesi, kas nodrošinātu VID prasībām atbilstoša Pakalpojuma sniegšanu.

Izstrādātājam jāapraksta Pakalpojuma kvalitātes nodrošināšanas un pārvaldības pasākumu (metožu) kopums, ko tas ir paredzējis izmantot Pakalpojuma kvalitātes nodrošināšanai.

1. **Kvalitātes kontrole un verifikācija** **(Obligāta)**

Pakalpojuma sniegšanas laikā Izstrādātājam ir jāveic dokumentācijas un programmkoda kvalitātes kontrole, jānodrošina preventīvās un korektīvās darbības, kā arī jāuztur pieraksti par dokumentācijas un programmkoda verifikāciju pirms tā nodošanas Pasūtītājam. Pēc Pasūtītāja pieprasījuma Izstrādātājam ir jānodrošina iespēja Pasūtītājam iepazīties ar dokumentācijas un programmkoda verifikācijas pierakstiem.

Izstrādātājam tehniskajā piedāvājumā ir jāapraksta dokumentācijas un programmkoda kvalitātes nodrošināšanas plāns.

1. **Versiju un konfigurāciju pārvaldība**  **(Obligāta)**

Izstrādātājam jānodrošina konfigurāciju un versiju pārvaldība saskaņā ar līguma projekta 0.2.0.pielikuma 1.2. un 1.3.apakšpunktiem.

Izstrādātājam tehniskajā piedāvājumā ir jāapraksta konfigurāciju un versiju pārvaldības principi un rīki.

## Vispārējas prasības Pakalpojumam

1. **Uzturēšanas un pilnveidošanas periods** **(Obligāta)**

Izstrādātājam ir jānodrošina Pakalpojuma sniegšana līdz brīdim, kamēr iestājas viens no šādiem nosacījumiem:

1. ir pagājuši 36 (trīsdesmit seši) mēneši no līguma spēkā stāšanās dienas;
2. ir izlietota līguma projektā noteiktā līguma kopējā summa.
3. **Pakalpojuma pieejamība (Obligāta)**

Izstrādātājam jānodrošina Pakalpojuma pieejamība Pasūtītāja darba dienās no pirmdienas līdz ceturtdienai no plkst. 8.15 līdz plkst.17.00, piektdienās no plkst.8.15 līdz plkst.15.45. Ja Pasūtītājs nosūta pieteikumu ārpus Pasūtītāja darba laika, tad reakcijas laikā tiek skaitīts tikai Pasūtītāja darba laiks.

Pakalpojuma ietvaros komunikācijai tiks izmantoti šādi komunikācijas kanāli – tālrunis, e-pasts, videokonferenču rīki, IPPV un ISIPS tiešsaistes savienojums un klātiene.

Izstrādātājam ir jānodrošina visi norādītie komunikācijas kanāli, tomēr Izstrādātājs, vienojoties ar Pasūtītāju, var noteikt primāri izmantojamo komunikācijas kanālu.

1. **Pakalpojuma saturs** **(Obligāta)**

Pakalpojuma sniegšanas laikā ir jānodrošina vismaz:

1. sistēmu darbības problēmu izpēte un novēršana;
2. VID datu labojumu veikšanu, ja datu bojājumi radušies piegādātās programmatūras kļūdu vai nepilnību dēļ;
3. pilnveidojumu un izmaiņu realizēšana;
4. konsultāciju sniegšana;
5. dokumentācijas aktualizēšana atbilstoši veiktajām izmaiņām sistēmās.

## Pieejamības un veiktspējas prasības

1. **Pieejamība** **(Obligāta)**

Sistēmai jānodrošina maksimāla pieejamība (Sistēmai ir jābūt pieejamai lietotājiem 24 stundas diennaktī, 7 dienas nedēļā) lietotājiem un tādu Sistēmas arhitektūras kvalitāti, lai tās darbība ir stabila un to Nodevumu uzstādīšanu ir iespējams veikt bez vai ar minimāliem Sistēmas darbības pārtraukumiem. Izstrādātāja darbības vai bezdarbības dēļ Sistēmas darbības pārtraukumi kopumā nedrīkst pārsniegt 12 (divpadsmit) stundas 12 (divpadsmit) kalendāro mēnešu laikā. Vienas atsevišķas dīkstāves gadījums nedrīkst pārsniegt 30 (trīsdesmit) minūtes VID darba laikā un 2 (divas) stundas pārējā laikā. Darbības pārtraukumu laikā ieskaita plānotās un neplānotās dīkstāves, bet neieskaita gadījumus, kad darbības pārtraukums ir noticis no Izstrādātāja neatkarīgu iemeslu dēļ. Sistēmas 12 (divpadsmit) mēnešu perioda darbības pārtraukumu laikā ieskaita arī visas atsevišķās dīkstāves, par kurām piemērots līguma 12.1.9.apakšpunktā noteiktais līgumsods, kas paredzēts par pieļaujamo vienas atsevišķas dīkstāves gadījuma stundu skaita pārsniegšanu.

1. **Veiktspēja** **(Obligāta)**

Jānodrošina stabila VIDISS darbība un šādas minimālās veiktspējas prasības pie nosacījuma, ka vienlaicīgo pieprasījumu skaits 1 sekundē ir ne mazāks par 20 pieprasījumiem:

| **Veids**  **Izmērs** | **līdz 50 KB** | **no 50 KB līdz 2 MB** | **virs 2 MB** |
| --- | --- | --- | --- |
| **Sinhronajiem pieprasījumiem** | Katra pieprasījuma apstrādes laiks VIDISS nav lielāks par 0,5 sek. | Katra pieprasījuma apstrādes laiks VIDISS nav lielāks par 5 sek. | Pieprasījuma apstrādei VIDISS jānotiek kā asinhronajam procesam. |
| **Asinhroniem pieprasījumiem 1** | Katra pieprasījuma apstrādes laiks VIDISS nav lielāks par 0,5 sek. | Katra pieprasījuma apstrādes laiks VIDISS nav lielāks par 5 sek. | n/a |

1Ņemot vērā, ka asinhronais pieprasījums sastāv no vairākiem sinhronajiem pieprasījumiem (pieprasījuma ievietošanā un atbildes saņemšanā), tad katra sinhronā pieprasījuma apstrādes laiks VIDISS nav lielāks par norādīto.

Asinhronajiem pieprasījumiem jānodrošina iespēja saņemt ziņojumu par pieprasījuma atbildes izveidošanu.

## Prasības pieteikumu apstrādei

1. **Pasūtītāja un Izstrādātāja sadarbības kārtība** **(Obligāta)**

Pakalpojuma aktivitātes var ierosināt gan Pasūtītājs, gan Izstrādātājs.

Visi problēmu ziņojumi un izmaiņu pieprasījumi (turpmāk – pieteikumi) līguma darbības laikā tiks pieteikti, izmantojot VID informācijas sistēmas izmaiņu pārvaldības sistēmu (ISIPS), saskaņā ar līguma projekta 0.1.0.pielikumā aprakstīto kārtību. Līguma izpildes laikā tiesības noteikt pieteikuma prioritāti (kritiska, steidzama vai parasta) ir attiecīgajām Pasūtītāja pilnvarotajām personām.

1. **Reakcijas laiks uz pieteikumu** **(Obligāta)**

 Reakcijas laikā Izstrādātājam jānodrošina pieteikuma izpēte, klasifikācija un atbildes sniegšana – reakcijas laiki (stundās), par pieteikumā norādītās problēmas cēloni un novēršanas laiku vai izmaiņu pieprasījuma realizēšanai prognozējamo darbietilpību un realizēšanai nepieciešamo laiku saskaņā ar līguma projekta 0.1.0.pielikuma 7.punktā noteikto.

1. **Pieteikumu risināšana garantijas nodrošināšanas pakalpojuma ietvaros (Obligāta)**

Izstrādātājam jānodrošina līguma 0.1.0.pielikumā aprakstītā pieteikumā aprakstītās problēmas novēršanas kārtība. Garantijas nodrošināšanas ietvaros Izstrādātājs bez maksas risina pieteikumu visiem pieejamajiem līdzekļiem, t.sk. nodrošina pieteikumu – problēmziņojumu izpēti, novērtēšanu un problēmziņojumā norādītās problēmas novēršanu, savukārt VID visiem pieejamajiem līdzekļiem sniedz pieteikuma risināšanai nepieciešamo papildus informāciju. Pieteikumu risināšanā jāievēro šīs specifikācijas prasības.

1. **Pieteikumu risināšana uzturēšanas pakalpojuma nodrošināšanas ietvaros (Obligāta)**

 Izstrādātājam jānodrošina līguma 0.1.0.pielikumā aprakstītā pieteikumā aprakstītā problēmas novēršanas kārtība. Uzturēšanas pakalpojuma nodrošināšanas ietvaros Izstrādātājs risina pieteikumu visiem pieejamajiem līdzekļiem, savukārt VID visiem pieejamajiem līdzekļiem sniedz pieteikuma risināšanai nepieciešamo papildus informāciju. Pieteikumu risināšanā jāievēro šīs specifikācijas prasības.

1. **Pieteikumu eskalācija Pakalpojuma sniegšanas ietvaros (Obligāta)**

 Pakalpojuma sniegšanas laikā Izstrādātājam nekavējoties jāinformē VID, ja pieteikumā risināšanas gaitā tiek konstatēts, ka pieteikumā aprakstītās problēmas novēršanai vai aprakstītā izmaiņu pieprasījuma realizācijai nepieciešama standartprogrammatūras, kura tiek izmantota Sistēmas darbības nodrošināšanā, ražotāja iejaukšanās, un pieteikumu nepieciešams eskalēt attiecīgajam ražotājam. Eskalētais pieteikums tiek risināts atbilstoši VID un attiecīgā ražotāja noteikumiem.

1. **Problēmu vadība** **(Obligāta)**

Izstrādātājam ir jānodrošina problēmu ziņojumu pārvaldība saskaņā ar līguma projekta 0.1.0.pielikumā aprakstīto sadarbības kārtību un 0.2.0.pielikuma 1.6.apakšpunktu.

## Izmaiņu realizācijas prasības

1. **Izmaiņu vadība** **(Obligāta)**

Izstrādātājam jānodrošina izmaiņu vadība saskaņā ar līguma projekta 0.1.0.pielikumā aprakstīto sadarbības kārtību un 0.2.0.pielikuma 1.4.apakšpunktu.

Izstrādātājam jāveic izmaiņu pieprasījuma izpēte, izmaiņu izstrāde (t.sk. attiecīgās dokumentācijas aktualizēšana, t.i. labošana, papildināšana utt.), testēšana un piegāde, pamatojoties uz Pasūtītāja prasībām, apstiprināto programmatūras prasību specifikāciju un apstiprināto PPA.

Par izmaiņu pieprasījumu nevar uzskatīt programmatūras prasību un projektējuma kļūdas vai nepilnības, kuras saskaņā ar labu industriālo praksi, Izstrādātājam bija savlaicīgi jāidentificē.

Pieprasīto programmatūras izmaiņu piegādē Izstrādātājam ir jāpiegādā attiecīgās dokumentācijas aktualizētā versija, kā arī piegādes pakotnei jāpievieno apraksts, kurā apkopoti visi konkrētajā piegādē realizētie izmaiņu pieprasījumi un kļūdu labojumi (ja tādi veikti).

Izstrādātājam tehniskajā piedāvājumā ir jāapraksta izmaiņu vadības sistēma un procedūras, kas tiek pielietotas Izstrādātāja uzņēmumā, atspoguļojot sadarbību ar Pasūtītāju.

1. **Darbietilpības novērtēšanai izmantotās Izstrādātāja metodes** **(Obligāta)**

Izstrādātājam detalizēti jāapraksta Pakalpojuma ietvaros paredzamo darbu darbietilpības novērtēšanas (aprēķināšanas) metode un risinājums speciālistu veikto darbu apjoma (patērētā laika) uzskaitei, kuru Izstrādātājs apņemas izmantot līguma izpildes laikā (jāpievieno piedāvājumam).

Izstrādātājam jāizmanto vismaz viena formālā metode, balstoties uz eksperta metodi.

1. **Standartprogrammatūras uzturēšanas prasība (Obligāta)**

 Pakalpojuma sniegšanas laikā Izstrādātājam nekavējoties jāinformē Pasūtītājs, ja tiek izdoti Sistēmas darbības nodrošināšanā izmantotās standartprogrammatūras jauninājumi vai kritiskie ielāpi, kuri var ietekmēt sistēmu darbību.

 Gadījumā, ja, lai nodrošinātu standartprogrammatūras, kura tiek izmantota Sistēmas darbināšanā, jauninājumu vai kritisko ielāpu uzstādīšanu Pasūtītāja testa/produkcijas vidē, nepieciešamas izmaiņas Sistēmā, Izstrādātājs iesniedz Pasūtītājam izvērtējumu par šādu izmaiņu darbietilpību saskaņā ar līguma 0.1.0.pielikumā “Sadarbības kārtība” aprakstīto kārtību. Ja standartprogrammatūras jauninājums vai kritiskais ielāps ir kritisks Sistēmas un/vai saistīto VID IS drošībai, Izstrādātājam jāiesniedz izvērtējums īsākā laikā, abpusēji vienojoties ar Pasūtītāju.

1. **Mērogojamība** **(Obligāta)**

 Sistēmas mērogošanu ir jānodrošina jaunai funkcionalitātei tādā veidā, ka tai jāvar darboties neatkarīgi no iepriekš izstrādātās funkcionalitātes (prasības mērogošanas pasākumi nav jānodrošina esošajai funkcionalitātei), turklāt jaunai funkcionalitātei būtu jāvar darboties bez papildu licencēm.

1. **Mērogojamības piemērojamība (Obligāta)**

Sistēma jāpilnveido un jāuztur, nodrošinot mērogošanu bez papildu izstrādes darbiem, un lai būtu iespējams palielināt Sistēmas veiktspēju, pievienojot papildus nepieciešamās standartprogrammatūras licences un aparatūru, tā, lai nerastos Sistēmas un/vai VID IS darbības traucējumi.

1. **Sistēmas darbība divos datu centros (Obligāta)**

Sistēma jāpilnveido un jāuztur tā, lai būtu iespējams darbināt Sistēmu divos datu centros.

1. **Sistēmas darbība klasterī (Obligāta)**

Sistēma jāpilnveido un jāuztur tā, lai nākotnē būtu iespējams palielināt Sistēmas un VID IS veiktspēju, darbinot to klasterī ar slodzes līdzsvarošanu *(load balancing)* paplašināšanas iespējām un redundances neatkarīgi no fizisko serveru skaita.

1. **Sistēmas darbības neatkarība no atsevišķa moduļa kļūmes (Obligāta)**

Sistēma jāpilnveido un jāuztur tā, lai jebkura viena moduļa kļūmes rezultātā nenotiek pilnīga Sistēmas un/vai VID IS darbības apstāšanās *(no single point of failure)*. Pieļaujama Sistēmas pakalpojumu kvalitātes pasliktināšanās uz laiku, kas nepieciešams kļūmes un kļūmes seku novēršanai.

1. **Sistēmu un to lietojumprogrammu modularitātes prasības** **(Obligāta)**

Izstrādātāja darbības rezultātā sistēmās nedrīkst mazināties esošā modularitāte. Par moduli tiek uzskatīts sistēmas funkcionālais apgabals, kas nodrošina loģisko funkciju kopumu veikšanu neatkarīgi no citiem moduļiem.

1. **Prasības pārnesamībai** **(Obligāta)**

Ja sistēmās tiek realizēta jauna funkcionalitāte un tā tiek realizēta, papildinot standartprodukta funkcionalitāti, papildinājumiem jābūt veidotiem tā, lai būtu iespējams bez izmaiņām pārnest šo funkcionalitāti uz jaunāku standartprodukta versiju.

1. **Neparedzēto kļūdu apstrāde** **(Obligāta)**

Pilnveidojot sistēmas, jānodrošina neparedzētu kļūdu apstrāde un žurnalēšana, saglabājot visu pieejamo ar kļūdu saistīto informāciju. Jānodrošina sistēmu notikumu žurnalēšana, uzkrājot datus par kļūdainiem sistēmu notikumiem (neskaitot paredzēto loģisko validāciju apstrādes laikā identificētās datu kļūdas).

Atbilstoši kļūdu žurnāla uzstādījumiem, jānodrošina iespēja nosūtīt ziņojumu par kļūdu sistēmas administratoram.

1. **Pieteikumu eskalācija (Obligāta)**

Gadījumos, kad pieteikuma par standartprogrammatūras darbības traucējumiem un/vai kļūdām un nepilnībām risināšanas gaitā tiek konstatēts, ka pieteikumā aprakstītās problēmas novēršanai nepieciešama standartprogrammatūras Izstrādātāja (ražotāja) iejaukšanās, tas tiek saskaņots ar Pasūtītāju, un pieteikums tiek eskalēts attiecīgajam ražotājam.

Tālāk pieteikums tiek risināts atbilstoši Pasūtītāja un attiecīgā ražotāja noteikumiem.

1. **Kļūdas paziņojumi** **(Obligāta)**

Sistēmās jāattēlo klasificēts kļūdas paziņojums (kļūda, brīdinājums, informācija) ar detalizētu aprakstu un iespējamām turpmākām darbībām.

Kļūdu paziņojumi ir jāveido tā, lai sistēmu programmatūra lietotājam nesniedz informāciju, kas varētu apdraudēt Pasūtītāja IS drošību, tai skaitā, nepieļaut iespēju lietotājam veikt analīzi par kļūdas un veikto pārbaužu raksturu. Kļūdas situācijās lietotājam ir jāparāda minimāli nepieciešamo informāciju, detalizētu tehnisko informāciju nosūtot sistēmas administratoram un veicot informācijas ierakstīšanu sistēmas žurnālā, lai pārāk detalizēti kļūdu paziņojumi neļautu lietotājam iegūt nevēlamu informāciju par izmantotajām tehnoloģijām, Pasūtītāja IS arhitektūru un veiktajām drošības pārbaudēm, kas varētu atvieglot tālākos uzbrukumus Pasūtītāja IS.

1. **Datu dzēšanas brīdinājums** **(Obligāta)**

Pilnveidojot sistēmas, jebkādu datu dzēšanas gadījumā jāpieprasa lietotāja apstiprinājums ieraksta dzēšanai.

1. **Informācijas iekšējās integritātes nodrošināšana** **(Obligāta)**

Jānodrošina informācijas integritāte no biznesa loģikas viedokļa. Lai nodrošinātu informācijas integritāti, jāveic datu validācija gan lietotāja, gan ārējās saskarnes, gan datubāzes līmenī.

1. **Prasība Sistēmas pilnveidošanai un uzturēšanai (Obligāta)**

Sistēma jāpilnveido un jāuztur tā, lai tiktu nodrošinātas šādas tehniskās prasības.

1. Servisu izstrādei Pakalpojuma sniegšanas laikā.
2. Visi servisi jāizstrādā saskaņā ar šīs specifikācijas prasībām un vadlīnijām (t.sk. Pasūtītāja XML shēmu izstrādes vadlīniju standartu, ar kuru Izstrādātājs var iepazīties klātienē Pasūtītāja telpās) un izmantojot Sistēmas esošo funkcionalitāti (piemēram, ADK, LDK). Pēc nepieciešamības var veikt ar Pasūtītāju saskaņotās izmaiņas Pasūtītāja XML shēmu izstrādes vadlīniju standartā.
3. Visus izstrādātos servisus jāvar izmantot atkārtoti.
4. Visi izstrādātie servisi jāpublicē OER, kā arī jāvar pārpublicēt VISS ar stingri definētiem *(strongly typed)* servisa kontraktiem.
5. Visiem izstrādātajiem ārējiem servisiem jābūt iespējai konfigurēt, vai kešatmiņa tiek izmantota un cik ilgi rezultāti tiek uzturēti kešatmiņā.
6. Par visiem izstrādātajiem servisiem jāvar pārskatāmā veidā iegūt statistiku par periodiem (dienā, mēnesī, ceturksnī, gadā un kopējo), to izsaukumu biežumu, cik ilgā laikā servisi sniedza atbildi, vai izsaukums beidzās ar kļūdu un citu informāciju, kas var būt nepieciešama servisu darba analīzei.
7. Integrācijai ar VISS, nodrošinot iespējas.
8. Centralizēti pievienot izsaukumiem atbilstošu autentifikācijas un autorizācijas informāciju.
9. VISS attīstības gadījumā (piemēram, pieprasījumu servisam publicēta jauna versija ar paaugstinātu drošības līmeni) centralizēti mainīt pieprasījumu servisa izsaukumu, nemodificējot realizētos izsaukumus VID IS.
10. Izsaucot asinhronus servisus, kontrolēt atbildes saņemšanu un nodošanu atpakaļ uz VID IS.
11. Jānodrošina savienojums ar Oracle, Informix, PostgreSQL, Microsoft SQL, SAP HANA DB, ar e-pasta serveriem, izmantojot SMTP, POP3 un IMAP protokolus, ārējiem rindu servisiem, JMS (Java Messaging Service), MSMQ (Microsoft Message Queuing), AMQP (Advanced Message Queuing Protocol).
12. **Serveru resursu klasterizācijas atbalsta nodrošināšana (Obligāta)**

Ja Pakalpojuma sniegšanas laikā jāveido jauna datu apmaiņas saskarne ar IS vai jāveic esošās datu apmaiņas saskarnes ar IS pārveide, tad ir jāveic veiktspējas testēšana kā arī jānodrošina serveru resursu klasterizācijas atbalsts veiktspējas palielināšanai.

1. **Prasības Sistēmas uzturamībai (Obligāta)**

Pakalpojuma sniegšanas laikā Sistēmas labākai uzturamībai jānodrošina šādi nosacījumi:

1) jābūt iespējai definēt un mainīt Sistēmas funkcionalitāti ar administratora definēto parametru palīdzību, piemēram, mainot konfigurācijas parametrus vai klasifikatoru vērtības;

2) Sistēma jāpilnveido un jāuztur tā, lai modificējot vienu Sistēmas moduli, pēc iespējas mazāk tiktu ietekmēti citi moduļi;

3) jāuztur pieejama dokumentācija, vadlīnijas un standarti, kas nepieciešami Sistēmas darbināšanai, t.sk. administrēšanai, jaunās funkcionalitātes pievienošanai.

## Testēšanas prasības

1. **Prasības testēšanai**

Izstrādātājam ir jānodrošina programmprodukta testēšana pirms programmprodukta iesniegšanas Pasūtītājam saskaņā ar līguma 0.2.0.pielikuma 1.5.apakšpunktu un šīs tehniskās specifikācijas prasībām.

Izstrādātājam jānodrošina sistēmu iekšējā testēšana atbilstoši savām procedūrām un testēšanas dokumentācijas sagatavošana.

Izstrādātājam ir jāapraksta, kāds būs testēšanas process, kādi būs testēšanas veidi (manuālā, automātiskā) un kādi testēšanas rīki tiks izmantoti, lai veiktu Nodevumu kvalitatīvu testēšanu; kāda testēšanas dokumentācija un kādā formātā tiks piegādāti testēšanas scenāriji, kā tiks saskaņoti un iesniegti testpiemēri, kad, kādā formātā un ar kādu saturu tiks iesniegti testu žurnāli.

1. **Izstrādātāja veiktie nodevumu testi**  **(Obligāta)**

Lai nodrošinātu Nodevuma atbilstību noteiktajām prasībām, Izstrādātājam ir jānodrošina Nodevumu iekšējā testēšana atbilstoši kādai no programmatūras izstrādes praksē pieņemtajām testēšanas metodoloģijām, un testēšanas dokumentācijas sagatavošana.

Izstrādātājam jānodrošina vismaz:

* 1. funkcionalitātes testēšana;
	2. integritātes testēšana;
	3. regresijas testēšana;
	4. drošības testēšana;
	5. veiktspējas, ātrdarbības un slodzes testēšana.

Testēšanu veic Izstrādātājs ar saviem resursiem, neiesaistot Pasūtītāju, pirms Nodevuma iesniegšanas, lai pārliecinātos, ka Nodevums ir gatavs akcepttestēšanai.

Programmatūras Nodevumi ir jāiesniedz kopā ar Izstrādātāja veiktās testēšanas dokumentāciju.

Veicot sistēmas laidienu piegādi, ir jāveic visu iepriekš piegādāto sistēmas daļu testēšana, ieskaitot to sistēmas daļu atkārtotu testēšanu, kas netika modificētas, ar mērķi pārliecināties, ka veiktās modifikācijas nav negatīvi ietekmējušas līdz šim izstrādātās sistēmas daļas.

Izstrādātājam tehniskajā piedāvājumā jāapraksta, kādi testēšanas veidi, metodes un rīki tiks izmantoti Nodevumu testēšanai, kādā formātā un ar kādu saturu tiks iesniegta testēšanas dokumentācija.

1. **Funkcionālā testēšana**  **(Obligāta)**
2. testpiemēros jāiekļauj visu programmatūras prasību specifikācijā/aprakstā iekļauto funkciju (prasību) pārbaude. Testpiemēros jāiekļauj gan „pozitīvie” (ievadīti korekti dati - mērķis ir pārbaudīt vai sistēmas programmatūras funkcionalitāte strādā korekti), gan „negatīvie” (ievadīti kļūdaini dati - mērķis ir pārbaudīt sistēmas programmatūras darbaspēju un korektu apstrādi kļūdu un problēmsituāciju gadījumā) piemēri.
3. testpiemēros jānorāda gan ievaddati, gan sagaidāmie rezultāti.
4. testēšanas scenārijos ir jāiekļauj visu darba plūsmas zaru pārbaude.
5. **Akcepttestēšana**  **(Obligāta)**

Pasūtītājs sagatavos sistēmas akcepttestēšanas vidi un veiks akcepttestēšanu saskaņā ar testēšanas dokumentāciju.

Izstrādātājam ir jānodrošina akcepttestēšanas vides sagatavošanai un akcepttestu norisei nepieciešamās konsultācijas.

Balstoties uz Pasūtītāja iesniegtajiem testēšanas protokoliem un problēmziņojumiem, Izstrādātājam jānovērš akcepttestēšanas laikā identificētās problēmas.

Izstrādātājam jāsagatavo un jāiesniedz Pasūtītājam testēšanas pārskats (Izstrādātājam ir jāveido plānoto testēšanas darbību rezultātu kopsavilkums un jānodrošina novērtējums, balstoties uz iegūtajiem rezultātiem).

Līguma darba rezultātu akcepttestēšanas kārtība jāveic saskaņā ar līguma 0.3.0. pielikumā aprakstīto kārtību.

1. **Funkcionalitātes demonstrācija** **(Obligāta)**

Sistēmas funkcionalitātes demonstrācijas mērķis ir pārliecināties, ka sistēma atbilst Pasūtītāja prasību analīzes laikā definētiem biznesa procesiem un sistēma pilda biznesa procesu nodrošināšanai nepieciešamo funkcionalitāti (sistēmas funkcionalitātes demonstrācijas laikā pieļaujama atsevišķu funkciju nekorekta darbība, ja tā netraucē Pasūtītājam pārliecināties par funkcionalitātes darbību pēc būtības). Demonstrācijas laikā Pasūtītājs neveic sistēmas akcepttestēšanu. Demonstrācija var notikt Izstrādātāja vidē.

Sistēmas funkcionalitātes demonstrācija veicama pēc Pasūtītāja pieprasījuma.

Atbilstoši sistēmas funkcionalitātes demonstrācijas laikā Pasūtītāju identificētiem nepieciešamiem papildinājumiem/ nepilnībām/ priekšlikumiem/ ierosinājumiem, Izstrādātājam ir jāveic izstrādātās un apstiprinātās programmatūras dokumentācijas papildināšana un/vai atjaunošana (sistēmas funkcionalitātes demonstrācijas laikā Pasūtītājs neizvirzīs prasību analīzes laikā definētām prasībām pretrunīgas prasības).

Izstrādātājam jāveic atjaunotās dokumentācijas atkārtota saskaņošana ar Pasūtītāju. Pēc dokumentācijas apstiprināšanas Izstrādātājam ir jāveic nepieciešamās izmaiņas Nodevumā.

1. **Veiktspējas, ātrdarbības un slodzes testēšana (Obligāta)**

Daudzlietotāju režīma veiktspējas, ātrdarbības un slodzes testēšanai ir jāsimulē sistēmas darbību:

1. nominālas noslodzes apstākļos (šī testa ietvaros ir jāparāda, ka sistēma var izpildīt noteiktās ātrdarbības prasības nominālas noslodzes apstākļos);
2. maksimālas noslodzes apstākļos (pakāpeniski paaugstinot noslodzi, nosakot slieksni, kad veiktspējas prasības vairs netiek izpildītas vai arī līdz sistēmas darbības atteicei).

Papildus Izstrādātājam jānodrošina:

1. stabilitātes testēšana (šī testa ietvaros ir jāpārbauda sistēmas darbības stabilitāte to ilgstoši darbinot pie dažādām noslodzēm, piemēram, nominālas noslodzes).
2. kapacitātes testēšana (šī testa ietvaros ir jāpārbauda sistēmas spēju robežas pie dotās tehniskās konfigurācijas).
3. mērogojamības testēšana (šī testa ietvaros ir jānoskaidro sistēmas mērogojamības iespējas).

Noslodzes nosacījumi ir jādetalizē programmatūras prasību specifikācijā.

Pirms slodzes testēšanas Izstrādātājam ar Pasūtītāju jāsaskaņo precīzi testa scenāriji un slodzes testa izpildes nosacījumi, kā arī kritēriji, pēc kuriem tiek akceptēta Sistēmas darba spēja pie iepriekš definētās slodzes.

1. **Drošības testēšana** **(Obligāta)**

Drošības testēšanas mērķis ir pārbaudīt sistēmas noturību pret nesankcionētu pieeju un uzbrukumiem.

Vienlaikus gan slodzes testa laikā, gan veicot drošības un funkcionālos testus, kas simulē dažādas kļūdas uz darbības atteikumu vērstas darbības, jāvērtē sistēmas darbības stabilitāte un drošība.

Izstrādātājam ir jānovērš testēšanas laikā atklātie defekti un jāiesniedz Pasūtītājam testēšanas dokumentācija. Izstrādātājs var Pasūtītājam iesniegt neatkarīgā audita rezultātus, vienojoties par neatkarīgā auditora kvalifikāciju.

## Nodevumu piegādes un uzstādīšanas prasības

1. **Darbu un nodevumu vispārīgā atbilstība (Obligāta)**

 Izstrādātājam Pakalpojuma ietvaros ir jāveic darbi un jāpiegādā Nodevumi (dokumentācijas un programmkoda) saskaņā ar šīs specifikācijas prasībām, iepirkuma nosacījumiem, Latvijas Republikā spēkā esošo normatīvo aktu prasībām, Latvijas Republikas un starptautiskajiem programmatūras izstrādes standartiem.

1. **Pakalpojuma Nodevumu nodošanas-pieņemšanas kārtība** **(Obligāta)**

Izstrādātājam līguma darba rezultātu nodošanas-pieņemšanas kārtība jāveic saskaņā ar līguma projekta 0.3.0. pielikumā aprakstīto kārtību.

1. **Nodevumu atbilstība standartiem**  **(Obligāti)**

Izstrādātājam ir jānodrošina Nodevumu atbilstība līguma projekta 0.5.0. pielikumā noteiktajiem standartiem.

1. **Programmatūras Nodevumu saturs un piegāde**

Programmatūras Nodevumā ietilpst: sagatavotā programmatūra komplektā ar pavaddokumentiem (var saturēt projektējuma dokumentāciju (PPS, PPA, izmaiņu projektējuma apraksts, algoritmu apraksts), programmatūras pirmkodus, instalācijas instrukciju, instalācijas pakotni ar programmatūras izpildkodiem un datubāzes skriptiem, datubāzes modeli un datubāzes struktūras aprakstu, Helpfailu, lietotāja un administratora dokumentāciju, testu projektējuma specifikāciju, testpiemēru specifikāciju, testēšanas kopsavilkuma pārskatu).

Programmatūras Nodevums jāpiegādā uzstādīšanai gan Pasūtītāja testa vidē, gan Pasūtītāja produkcijas vidē, ar norādi par programmatūras Nodevuma instalēšanas paketes uzstādīšanas vidi, ja tehniski nav iespējams piegādāt programmatūras Nodevuma instalēšanas paketi, kas izmantojama abās vidēs. Programmatūras instalēšanas paketei jābūt “inkrementālai”, t.i. tās uzstādīšana ir veicama uz iepriekš piegādātas versijas. Programmatūras Nodevumi nedrīkst ietekmēt datubāzē jau esošos datus, ja vien tas nav iepriekš īpaši saskaņots vai nav Nodevumu objekts. Gadījumos, ja tiek mainīta datubāzes struktūra, jāpiegādā arī atbilstošie datu migrācijas skripti.

Visiem Nodevumiem ir jānodrošina versiju identifikācija un kontrole.

Nodevumi jāpiegādā saskaņā ar šajā specifikācijā, līguma projekta 4, 5., 6., 7.punktā, 0.1.0.pielikumā “Sadarbības kārtība”, 0.2.0.pielikumā “Sistēmu uzturēšanas un pilnveidošanas kvalitātes un pārvaldības tehniskās prasības” un 0.3.0.pielikumā “Līguma darba rezultātu nodošanas-pieņemšanas kārtība un akcepttestēšanas kārtība” noteikto kārtību.

1. **Prasības programmatūras nodevumiem** **(Obligāta)**

Piegādātā programmatūras pirmkoda kvalitātei ir jābūt pietiekošai, lai Pasūtītāja vai tā nolīgts trešās puses kvalificēts personāls varētu nodrošināt programmatūras turpmāko uzturēšanu, modificēšanu, paplašināšanu, kā arī iespējamo migrēšanu.

Izstrādātājam jāpiegādā Pasūtītājam programmatūras pirmkods tādā formā, lai to (visu vai konkrētu daļu – saskaņā ar Izstrādātāja norādījumiem) bez modifikācijām var atvērt Pasūtītājs savā testa vidē un nokompilēt (ja piegādātais programmatūras pirmkods ir kompilējams).

Programmatūras pirmkodam jāsatur komentāri latviešu valodā, kas ir viegli saprotami atbilstošas kvalifikācijas speciālistiem bez pirmkoda autora palīdzības.

Izstrādātājam jāpiegādā Pasūtītājam arī ar piegādāto pirmkodu saistīto dokumentāciju – shēmas, grafikus, utt. izejas failu veidā, kā arī pārveidotus \*pdf faila formātā.

Izstrādātājam tehniskajā piedāvājumā ir jāapraksta programmatūras dokumentēšanas principi, apjoms un jāsniedz programmatūras dokumentācijas un pirmkodu piemēri.

1. **Prasības dokumentācijas Nodevumiem** **(Obligāta)**

Darbu izpildes rezultātā izveidotā vai aktualizētā, t.i., labota un/vai papildināta, dokumentācija ir jāpiegādā nodevuma ietvaros. Ja dokumentācija tiek aktualizēta, to jāintegrē attiecīgā dokumenta pēdējā (aktuālajā) versijā, saglabājot izmaiņu trasējamību (*Track Changes* režīmā, kā arī Izmaiņu lapā), tādējādi novēršot dokumentācijas sadrumstalošanos.

1. **Nodevumu trasējamība** **(Obligāta)**

Izpildītājam jānodrošina šādu Nodevumu trasējamība:

1) PPS definēto prasību trasējamība ar konkrētā Vienošanās protokolā noteiktām prasībām;

2) PPA trasējamība ar PPS definētām prasībām (prasību numuriem);

3) testpiemēru trasējamība ar PPS un PPA definētām prasībām (prasību numuriem).

1. **Programmatūras uzstādīšana Pasūtītāja akcepttestēšanas vidē**  **(Obligāta)**

Pēc programmatūras Nodevuma saņemšanas Pasūtītājs veiks sistēmas programmatūras uzstādīšanu un konfigurēšanu akcepttesta vidē. Izstrādātājam ir jānodrošina nepieciešamais atbalsts Pasūtītāja darbiniekiem sistēmas programmatūras uzstādīšanas un konfigurēšanas laikā akcepttesta vidē.

1. **Programmatūras uzstādīšana produkcijas vidē**  **(Obligāta)**

Pēc akcepttestēšanas pabeigšanas Pasūtītājs veiks sistēmas programmatūras uzstādīšanu un konfigurēšanu produkcijas vidē. Izstrādātājam ir jāpiegādā pēdējās atkļūdotās programmatūras un dokumentācijas versijas, kā arī jānodrošina nepieciešamais atbalsts (arī klātienē) Pasūtītāja darbiniekiem sistēmas uzstādīšanas un konfigurēšanas produkcijas vidē laikā.

Sistēmu uzturēšanas un pilnveidošanas ietvaros Izstrādātājam nepieciešams nodrošināt augstu sistēmas Nodevumu kvalitāti, lai sistēmas darbība ir stabila.

## Drošības prasības

1. **Drošības prasības uzturēšanas un pilnveidošanas nodrošināšanas laikā**  **(Obligāta)**

Saskaņā ar līguma 0.7.0. pielikumā noteiktajām prasībām.

## Garantija

1. **Garantijas periods un apjoms** **(Obligāta)**

Izstrādātājam ir jānodrošina 24 (divdesmit četru) kalendāro mēnešu garantijas periods, skaitot no attiecīgā nodošanas-pieņemšanas akta abpusējas parakstīšanas dienas, saskaņā ar līguma projekta 9.punktu. Izstrādātājs var piedāvāt garāku garantijas nodrošināšanas termiņu.

Garantijas ietvaros Izstrādātājam jānodrošina bezmaksas kļūdu (programmatūrā, datubāzē utt.) novēršana, t.sk. jānovērš datu bojājumi, kas radušies Izstrādātāja apzinātas vai neapzinātas rīcības rezultātā, un kas apgrūtina sistēmas izmantošanu atbilstoši tehniskajai specifikācijai, kāda tā bijusi, nododot sistēmu ekspluatācijā.

1. **Garantijas saturs** **(Obligāta)**

Garantijai ir jāietver vismaz šādu darbību veikšana:

1. piegādātās programmatūras darbības traucējumu un/vai kļūdu un nepilnību diagnosticēšana, analīze un novēršana;
2. Pasūtītāja datu labojumu veikšana, ja datu bojājumi radušies piegādātās programmatūras (t.sk. trešās puses programmatūras) kļūdu vai nepilnību dēļ;
3. dokumentācijas aktualizēšana (t.i. labošana, papildināšana utt.) atbilstoši visiem garantijas nodrošināšanas ietvaros veiktajiem labojumiem;
4. konsultāciju sniegšanu saņemto risinājumu konfigurēšanā.
5. **Programmatūras darbības traucējumu un/vai kļūdu un nepilnību novēršanas termiņi un nosacījumi** **(Obligāta)**

Garantijas ietvaros Izstrādātājam ir jānovērš piegādātās programmatūras darbības traucējumi, ja tādi rodas, un kļūdas un nepilnības, ja tādas tiek atklātas, bez papildu maksas.

1. Šeit un turpmāk: zaļgans fons – VIDISS komponentes, zilgans fons – saistītie produkti, kas ir VID rīcībā, balts fons – VID un ārējo iestāžu IS (SC un SP). [↑](#footnote-ref-2)