Gregor Plantarič

Digitalno podpisal Gregor Plantarič
DN: c=SI, o=state authorities, ou=web-certificates, givenName=Gregor, sn=Plantarič, serialNumber=1237988714015, cn=Gregor Plantarič
Datum: 2022.09.05 11:59:24 +02'00'

VZDRŽEVANJE

PLATFORME ZA DISTRIBUCIJO STORITEV E-PRAVOSODJA

TEHNIČNA DOKUMENTACIJA IN OPIS STORITEV

Ljubljana, 31. 8. 2022

KAZALO VSEBINE:

1 Uvod ... 3
1.1 Obstoječe stanje ... 3
1.2 Cilj naročila storitev ... 3
2 Predmet naročila ... 4
3 Specifikacije naročila ... 4
4 Način izvajanja storitev ... 4
5 Izvedbene zahteve ... 5
6 Varstvo osebnih podatkov ... 6
7 Obračun storitev ... 6
8 Kadrovski in partnerski pogoji ... 6
8.1 Reference ponudnika ... 6
8.2 Strokovna usposobljenost kadrov ... 7
9 Avtorske pravice ... 9
10 Merilo ... 9
I PRILOGA 1: Opis sistema ... 10
II Seznam gradnikov z opisi ... 10
II.a KumuluzIntegration ... 11
II.b API Prehod ... 11
III Popis uporabljenih tehnologij in/ali morebitne dodatne opreme ... 11
IV Arhitektura sistema ... 12
V Varnostni in zaščitni mehanizmi ... 14

1 Uvod

1.1 Obstoječe stanje

Informacijski sistem Ministrstva za pravosodje (IS MP) izvaja predvsem namenske aplikacije, ki podpirajo poslovna področja MP. Na MP so takšna poslovna področja predvsem nacionalne in mednarodne kazenskopravne evidence ter druge evidence, ki jih je MP dolžno voditi po zakonu.

Značilnost poslovnih področij je vpetost in povezanost poslovanja MP z drugimi sistemi državne in javne uprave, mednarodnimi pravosodnimi institucijami, kot tudi z gospodarstvom in državljani. Učinkovita in uspešna informacijska podpora poslovnim področjem zahteva urejeno, standardno ter upravljano integracijo in distribucijo storitev z drugimi informacijskimi sistemi tako znotraj pravosodja kot z zunanjimi povezanimi sistemi. Posledica centralizacije državne informatike je selitev aplikacij v državni računalniški oblak (DRO), ki predstavlja nov tehnološki eko-sistem za izvajanje IS MP tako, da prevzema zagotavljanje infrastrukturnih zmogljivosti in kapacitet za informacijsko podporo poslovnim področjem MP.

Obstoječe ter predvidene aplikacije, ki jih izvaja informacijski sistem MP, zagotavljajo in potrebujejo informacijske storitve, ki jih ponujajo drugi sistemi oziroma aplikacije. Ti sistemi so predvsem:

- pravosodne institucije (MP, VDT, DO, URSIKS, UPRO, sodna oblast, VSRS),
- institucije države (druga ministrstva, upravne enote, centri za socialno delo …),
- zainteresirana javnost (notarji, izvedenci),
- mednarodne institucije (ECRIS, TCN) in
- državljani RS in EU (dostop do pravosodnih podatkov in informacij).

MP je zato v svoj informacijski sistem uvedlo Platformo za distribucijo storitev e-pravosodja (PDSeP), ki bo ustrezno naslovila sistemske oziroma aplikativne integracijske funkcionalnosti za vse nove IT rešitve MP, ki so sedaj v fazi razvoja. PDSeP je nameščen na infrastrukturi MJU, kjer bodo nameščene tudi vse IT rešitve MP.

Opis obstoječega sistema se nahaja v prilogi 1, ki je del te tehnične dokumentacije.

1.2 Cilj naročila storitev

Cilj naročila je zagotoviti:

- pregled nad delovanjem infrastrukture in storitev ter zagotavljanje razpoložljivosti,
- učinkovito, enotno, upravljano in varno integracijo ter distribucijo storitev, ki jih zagotavljajo obstoječi in predvideni IS MP,
- poenotenje integracijskih pristopov bo izboljšala integracija na osnovi uveljavljenih integracijskih vzorcev, ki bodo lahko izvedeni na PDSeP,
- nadzor in upravljanje integracij, njihovo ustrezno beleženje ter spremljanje,
- lažje, hitrejše, bolj standardno in enotno izvedbo integracij ter njihovo upravljanje,
- večjo transparentnost / poenotenje integracij, posebno s horizontalnimi gradniki MJU (npr.: pladenj),
- standardizacijo integracij na osnovi uveljavljenih in dokumentiranih integracijskih vzorcev,
- izboljšanje obvladljivosti in upravljanja potrebnih ter ponujenih storitev,
- zmanjšanje kompleksnosti aplikacij in posledično izboljšanje njihovih operativnih ter varnostnih lastnosti,
- nižanje operativnih stroškov, povezanih z aplikativno programsko opremo.

2 Predmet naročila

Predmet naročila je "Vzdrževanje Platforme za distribucijo e-storitev pravosodja" za obdobje dveh let, ki zajema:

- osnovno vzdrževanje,
- dopolnilno vzdrževanje - storitve izdelave integracij in ostale storitve po naročilu.

3 Specifikacije naročila

Obseg podpore in izvajanje storitev zajema storitev integracij ter redne in izredne preglede, vzdrževanje sestavov PDSeP ter ostala opravila na zahtevo naročnika:

storitev	obseg
Osnovno vzdrževanje	Zagotavljanje varnega in nemotenega delovanja platforme, vključuje: - spremljanje delovanja PDSeP, - analiziranje delovanja PDSeP in predlaganje morebitnih nadgradenj, - redno posodabljanje programske kode z varnostnimi popravki in sprotno odpravljanje zaznanih napak. Naročnik ocenjuje, da je za izvedbo storitev potrebnih do 16 **ur dela mesečno;** naročnik mesečno plačuje izvajalcu enak znesek (pavšal).
Dopolnilno vzdrževanje	Storitve po naročilu zajemajo vsaj: – razvoj novih integracij in objava na platformi, – pomoč pri uporabi platforme, – pomoč pri konfiguraciji uporabnikov, odjemalcev, registracija API-jev, – odprava napak v delovanju sistema, ki po vsebini in obsegu presegajo okvir storitev osnovnega vzdrževanja, – druge storitve po naročilu. Naročnik ocenjuje, da je za izvedbo storitev v obdobju dveh let potrebnih **do 1.600 ur dela**. Dela se bodo izvajala na poziv. Naročnik plača le dejansko opravljene ure.

4 Način izvajanja storitev

Osnovno vzdrževanje: Razpoložljivost ponudnikove ekipe: - dosegljivost po telefonu ali elektronski pošti ob delovnikih v času med 8. in 16. uro Mesečno poročilo vključuje: - mesečni pregled delovanja sistema in objavljenih integracij, - opis odpravljenih napak, - morebitni predlogi priporočenih ukrepov.
Storitve po naročilu:

V okviru izvedbe novih integracij po naročilu naročnika izvajalec:

- izvede testne mehanizme in preizkus,
- vključi nove integracije PDSeP v operativni sistem naročnika in izvede preizkus delovanja,
- sodeluje pri usposabljanju in nudenju pomoči uporabnikom PDSeP (konfiguracija uporabnikov, odjemalcev, registracija API-jev),
- zagotavlja, da so pravosodne aplikacije nameščene v okviru priporočil najboljših praks in standardov,
- za naročnika izvede predstavitev narejenega in če je potrebno tudi prenos znanja,
- izdela in preda dokumentacijo, vključno z vsemi potrebnimi kodami, navodili za uporabo ipd.

V okviru izvedbe storitev vzdrževanja po naročilu za odpravo napake naročnika izvajalec:

- sodeluje pri določitvi napake in jo v dogovorjenem času odpravi.

Odzivni časi za odpravo napak:

- 1 ura za kritične napake, ki preprečujejo ali onemogočajo obratovanje storitev,
- če sistem ni odziven oz. ni dosegljiv na daljavo mora izvajalec priti na lokacijo napake v roku 3 ur,
- naslednji delovni dan za nekritične napake.

Naročanje storitev po naročilu poteka na način, da naročnik in izvajalec predhodno dogovorita vsebino, obseg in roke posamezne aktivnosti, naročnik pa končni dogovor potrdi s pisnim naročilom po e-pošti.

Poročilo o opravljenih storitvah po naročilu:

- za posamezne storitve (integracij PDSeP) izvajalec pripravi prevzemni zapisnik delujoče integracije v testnem in produkcijskem okolju, ki ga podpišeta obe pogodbeni stranki. Zapisnik vsebuje opis opravljenih storitev in opredelitev porabe časa za posamezno storitev. Zapisnik se mora sklicevati na pripadajoče naročilo naročnika;

- za ostale storitve po naročilu (odprava napak ipd.) izvajalec po njihovi odpravi pripravi poročilo, ki vsebuje opis opravljenih storitev in opredelitev porabe časa za posamezno storitev ter morebitne predloge oziroma načrt, ki bo v največji možni meri prispeval k nemotenemu delovanju sistema PDSeP.

Poročilo se mora sklicevati na pripadajoče naročilo naročnika. Izvajalec lahko pripravi poročilo za vsako posamezno storitev ali pa v poročilo vključi več storitev, opravljenih v določenem časovnem obdobju.

5 Izvedbene zahteve

Med naročnikom in ponudnikom bo potekala komunikacija ter obveščanje po telefonu ali v elektronski obliki. Vsa komunikacija med naročnikom in izvajalcem mora potekati v slovenskem jeziku.

Izvedbena dela, ki ne spadajo v redne preglede in vzdrževanje predvidenih aplikacij oz. sestavov aplikacij, se začnejo izvajati po pisni ali elektronski potrditvi naročnika.

Za nemoteno delo in pravočasno pripravo poročil naročnik dodeli kontaktno osebo – tehničnega skrbnika pogodbe, ki bo izvajalcu nudil pomoč v primeru zagotovitve odgovorov na vprašanja. Vse ostale

podrobnosti in časovne razmejitve o izvedbi storitev bodo določene ter zapisane pred izvedbo posamezne storitve.

Med izvajanjem storitev zaradi samega izvajanja ne sme priti do prekinitve v delovanju informacijskega sistema. Če bi izvajalec s svojimi aktivnostmi lahko dosegel možnost zaustavitve delovanja ali onesposobitev sistema, mora nemudoma prenehati z vsemi aktivnostmi preizkusa in o tem nemudoma obvestiti kontaktno osebo naročnika ter počakati na nadaljnja navodila.

Za izdelke po naročilu izvajalec jamči garancijsko vzdrževanje v roku najmanj 12 mesecev. V okviru tega odpravlja napake, vzdržuje kodo in dokumentacijo sistema (tehnično in uporabniško).

6 Varstvo osebnih podatkov

Izvajalec za opravljanje storitev, ki so predmet specifikacij, ne bo imel dostopa do morebitnih zbirk naročnika, v katerih ta hrani osebne podatke, ravno tako pa mu to s strani naročnika ne bo smelo biti omogočeno.

Če se bo izvajalec pri opravljanju pogodbenih storitev slučajno, nenamerno seznanil s kakršnimikoli osebnimi podatki, ki jih hrani naročnik, bo ustavil vse aktivnosti v okviru izvajanja storitev in naročnika o tem nemudoma obvestil.

Naročnik in izvajalec morata pred kakršno koli obdelavo osebnih podatkov skleniti pogodbo o obdelavi osebnih podatkov v vsakem primeru, kjer bi izvajalec za nemoteno izvajanje storitev, ki so predmet specifikacij, vključeval obdelavo osebnih podatkov.

Vsi predstavniki izvajalca, ki bodo opravljali storitve za naročnika v imenu in za račun izvajalca, bodo pred pričetkom opravljanja storitev podpisali posebno izjavo o varstvu osebnih podatkov, ki je del razpisne dokumentacije. Kopijo izjave za vsakega posameznega predstavnika bo izvajalec poslal naročniku pred sklenitvijo pogodbe.

7 Obračun storitev

Naročnik bo za storitve osnovnega vzdrževanja plačeval izvajalcu pavšalni znesek na podlagi računa, ki ga bo izvajalec izstavil do 5. v mesecu za pretekli mesec.

Opravila na zahtevo naročnika se bodo obračunala po dejansko porabljenih urah, potrebnih za opravo naročene storitve. Za predmetne storitve bo izvajalec naročniku izstavil račun(e).

Rok plačila je 30. dan od prejema pravilno izstavljenega računa.

8 Kadrovski in partnerski pogoji

8.1 Reference ponudnika

Ponudnik mora imeti izkušnje pri podobnih poslih. Za opredelitev podobnega posla se štejejo informacijske rešitve, ki zadostijo »minimalni referenčni rešitvi«, ki je definirana kot informacijska rešitev z naslednjimi pogoji oz. lastnostmi:

1. vpeljava platforme za distribucijo storitev, ki izkazuje primerljiv obseg funkcionalnosti s platformo PDSeP,
2. rešitev predana in uvedena v produkcijsko rabo v zadnjih petih letih pred objavo tega javnega naročila,
3. rešitev uspešno deluje v produkcijski rabi že vsaj eno leto pred objavo tega javnega naročila,

4. ponudnik je izobrazil kadre naročnika ali sam izvajal storitve razvoja in objavljanja integracij na rešitvi v produkciji vsaj eno leto,
5. ponudnik je za to rešitev nudil storitve vzdrževanja v produkciji vsaj eno leto,

Ponudnik mora izkazati najmanj dva podobna posla, od katerih je vsaj pri enem skupna vrednost s predvidenim vzdrževanjem za obdobje pet let minimalno 80.000 EUR brez DDV.

Upoštevajo se samo referenčne rešitve (projekti), ki so na dan roka za prejem ponudb po tem javnem naročilu še vedno v produkcijski rabi.

Ponudnik izpolni Obrazec izjava o referenčnem poslu za vsak izkazan podoben posel.

8.2 Strokovna usposobljenost kadrov

Ponudnik mora za čas izvajanja tega javnega naročila zagotoviti sodelovanje projektne skupine z naslednjimi vlogami in ustrezno razpoložljivostjo:

1. arhitekt sistema,
2. razvijalec aplikacijskega in podatkovnega nivoja,
3. razvijalec predstavitvenega nivoja.

Navedeni kadri morajo biti s ponudnikom oz. partnerjem v ponudbi oz. podizvajalcem v rednem delovnem ali drugem pogodbenem razmerju (npr. podjemna ali avtorska pogodba) v času oddaje ponudbe in nato ves čas izvajanja projekta. Ponudnik lahko v skladu z 81. členom ZJN-3 glede pogojev v zvezi s strokovno usposobljenostjo kadra uporabi zmogljivosti drugih subjektov le, če bodo slednji dejansko delali na projektu.

Ponudnik mora zagotoviti vsaj tri različne osebe, kjer je vsaj ena oseba v vlogi arhitekta sistema, vsaj ena oseba v vlogi razvijalca aplikacijskega in podatkovnega nivoja ter vsaj ena oseba v vlogi razvijalca predstavitvenega nivoja.

Projektna skupina mora izpolnjevati naslednje minimalne pogoje:

1. Arhitekt sistema:
    a. aktivno znanje slovenskega jezika,
    b. delovne izkušnje: tri leta v zadnjih petih letih na področju načrtovanja informacijskih rešitev,
    c. posebna znanja in veščine:
        – načrtovanje večnivojske arhitekture,
        – načrtovanje rešitev po arhitekturnem vzorcu mikrostoritev,
        – načrtovanje rešitev v tehnologijah Java verzije osem (8) ali več, ali Java/Jakarta EE verzije sedem (7) ali več, ali Spring Framework verzije 4.0 ali več,
        – načrtovanje rešitev, ki uporabljajo relacijske podatkovne baze,
        – načrtovanje integracij po standardih REST in SOAP,
        – načrtovanje »single-page application« rešitev,
        – izkušnje z izvajalnim okoljem za vsebnike (npr. Docker)
    d. Ima enega izmed naslednjih certifikatov: "Oracle Certified Professional: Java SE Developer vsaj verzije 8", ali "Spring Certified Professional" ali ekvivalentno,
    e. reference: aktivno sodelovanje pri načrtovanju in izvedbi rešitev v vlogi arhitekta sistema pri dveh podobnih poslih.

2. Razvijalec aplikacijskega in podatkovnega nivoja:

    a. delovne izkušnje: tri leta v zadnjih petih letih na področju programiranja aplikacijskega in podatkovnega nivoja,

    b. posebna znanja in veščine:

        – razvijanje rešitev v večnivojski arhitekturi,
        – razvijanje rešitev po arhitekturnem vzorcu mikrostoritev ,
        – razvijanje v tehnologijah Java verzije osem (8) ali več, ali Java/Jakarta EE verzije sedem (7) ali več, ali Spring Framework verzije 4.0 ali več
        – razvijanje na relacijski podatkovni bazi.

    c. reference: vloga razvijalca aplikacijskega in podatkovnega nivoja pri dveh podobnih poslih

3. Razvijalec predstavitvenega nivoja:

    a. delovne izkušnje: tri leta v zadnjih petih letih na področju programiranja predstavitvenega nivoja v obliki »single-page application«,

    b. posebna znanja in veščine:

        – razvijanje v programskem jeziku JavaScript ali TypeScript,
        – razvijanje v tehnologiji Angular,
        – razvijanje predstavitvenega nivoja, ki uporablja aplikacijski nivo z arhitekturnim stilom REST oz. API-ji,

    c. reference: vloga razvijalca predstavitvenega nivoja sistema z uporabo navedenih posebnih znanj in veščin pri dveh podobnih poslih

Ponudnik izkaže **izpolnjevanje pogoja s predložitvijo naslednjih podatkov** za posamezen kader:

1. ime in priimek,
2. vloga oz. vloge na razpisanem projektu,
3. pogodbeno razmerje do ponudnika (zaposlen/v drugem pogodbenem razmerju pri/s ponudnikom/partnerjem v projektu/podizvajalcem z navedbo vrste pogodbenega razmerja ipd.),
4. delovne izkušnje (vsaj zahtevane),
5. posebna znanja in veščine (vsaj zahtevane),
6. za vsako (vsaj zahtevano) referenco:
    a. naročnik,
    b. opis projekta,
    c. vrednost projekta z DDV,
    d. obdobje izvajanja z datumom uvedbe v produkcijo,
    e. opis aktivnosti tega kadra na projektu,
    f. kontaktna oseba (ime in priimek) pri naročniku, ki lahko potrdi referenco kadra, s kontaktnimi podatki (telefon, e-pošta).
7. kjer je predvideno, da kader poseduje certifikat, veljajo, poleg naštetih certifikatov, tudi certifikati, katerih primerljivost izkaže ponudnik.

Izbrani ponudnik je dolžan naročnika sproti obveščati o vsaki kadrovski spremembi pri izvajanju storitev tega naročila glede na navedbe v ponudbi. Kot sprememba se štejejo morebitni dodatni kadri, ki bi opravljali predmetne storitve, kot tudi morebitna zamenjava v ponudbi prijavljenega kadra.

Dodatne oz. nadomestne osebe morajo izpolnjevati minimalne pogoje kadrovske usposobljenosti za posamezno vlogo in imeti enake ali boljše strokovne kvalifikacije, kot jih je ponudnik zagotovil ob oddaji

ponudbe. To strokovno usposobljenost kadra naročnik dokazuje z enakim naborom podatkov o dodatnem/novem kadru kot ob oddaji ponudbe za prijavljen in dopolnjen/nadomeščen kader. Izbrani ponudnik mora torej imeti ves čas izvajanja pogodbenih obveznosti na voljo kadre, ki izpolnjujejo vse zahtevane pogoje skladno s specifikacijami in merili naročila storitev. Za prenos znanja in vpeljavo v utečen proces dela na projektu poskrbi izbrani ponudnik na svoje stroške in na način, da zagotovi nemoteno kontinuiteto dela v skladu s terminskim načrtom projekta.

9 Avtorske pravice

Izvajalcu bo na njegovo zahtevo omogočena seznanitev z izvorno kodo, ki je shranjena v SVN repozitoriju na infrastrukturi MJU.

10 Merilo

Merilo za izbiro izvajalca je najcenejša ponudba v skladu s specifikacijami in izpolnjenimi kadrovskimi ter partnerskimi pogoji. Izvajalec se lahko prijavi s podizvajalcem.

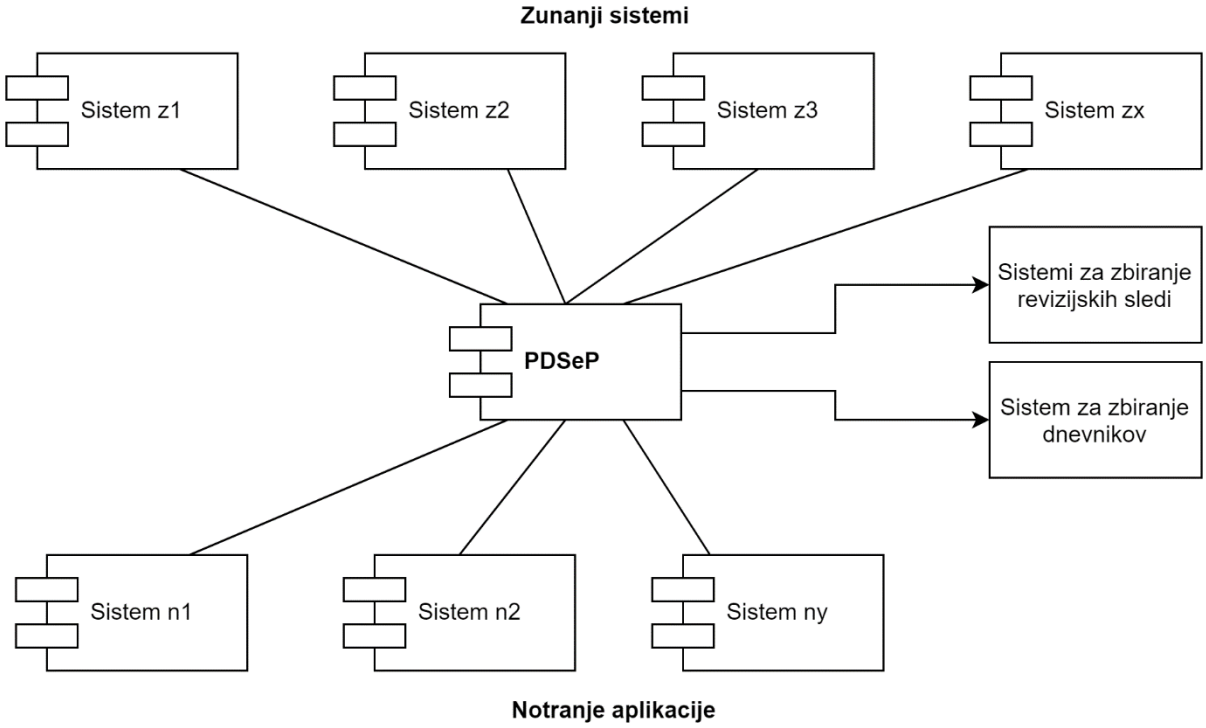
I PRILOGA 1: Opis sistema

Platforma za distribucijo storitev e-pravosodja (PDSeP) naslavlja sistemske oziroma aplikativne integracijske funkcionalnosti.

PDSeP nam namreč že omogoča, da se integracije ne bodo več izvajale točkovno, kot je tudi prikazano na sliki spodaj. Vsak integriran sistem (na sliki označena kot Sistem z1, Sistem z2…) se na platformo registrira oziroma objavi zgolj enkrat. Aplikacije ali sistemi, ki nato želijo klicati to storitev (na sliki označene kot Sistem n1, Sistem n2…) kot točko za izvajanje klicev do storitve uporabijo platformo PDSeP.

Nove integracije in komunikacija med IT sistemi in PDSeP bodo tipično realizirane skozi protokola SOAP ali REST, vendar je mogoče na nivoju PDSeP izpostaviti ali prožiti klice tudi po drugih protokolih, ki temeljijo na HTTP(S). V tem kontekstu je mogoče na PDSeP za integracijo definirati tudi transformacijo protokola, na primer SOAP v REST.

Čeprav bo smer izvajanja integracij tipično v smeri od sistemov notranjih aplikacij proti PDSeP in nato naprej proti zunanjem sistemu, nismo omejeni na zgolj ta integracijski vzorec. Posledično tudi povezave med sistemi in PDSeP na sliki niso predstavljene kot puščice, saj PDSeP podpira tudi asinhrone klice in periodično proženje integracij, ki se definirajo na nivoju PDSeP.



Slika 1 – Pregled povezav/odvisnosti s platformo PDSeP

II Seznam gradnikov z opisi

Integracijsko platformo sestavljajo naslednji gradniki:

- KumuluzIntegration,
- API prehod/i.

II.a KumuluzIntegration

Integracijska platforma KumuluzIntegration je namenjena upravljanju integracijskih API-jev in nadzoru ter upravljanju integracijskih storitev in komponent, kar vključuje integracijske mikrostoritve in API-je. KumuluzIntegration nudi vpogled v izvajanje integracijskih storitev in povezanih APIjev, ki so implementirane v poljubnem programskem jeziku, na poljubni platformi, klasično ali v obliki mikrostoritev. Integracijski API-ji so objavljeni v centralnem registru API-jev na KumuluzIntegration platformi. KumuluzIntegration podpira podrobno dokumentiranje integracijskih API-jev, definiranje operacij in končnih točk, ki jih izpostavlja integracijski API, upravljanje naročnin, pregled vitalnosti integracijskih API-jev, pregled metrik uporabe, pregled logov in upravljanje nastavitev integracijskih API-jev. KumuluzIntegration omogoča tudi upravljanje načinov dostopa do integracijskih API-jev preko planov uporabe. Integracijski API-ji so lahko javni, kar pomeni, da ne zahtevajo naročanje odjemalnih aplikacij, ali pa zasebni. Zasebni API-ji za uporabo zahtevajo naročnino odjemalne aplikacije, ki ob potrjeni naročnini prejme neko poverilnico (npr. API ključ), s katero se odjemalna aplikacija identificira API Prehodu, preko katerega odjemalne aplikacije dostopajo do integracijskih API-jev.

II.b API Prehod

API Prehod je komponenta, preko katere potekajo vsi dostopi do integracijskih API-jev. API prehod izvaja preverjanje API ključev in izvajanje politik dostopa. Politike dostopa omejujejo in nadzirajo dostop odjemalnih aplikacij do integracijskih API-jev. API prehod omogoča izvajanje naslednjih politik dostopa:

- **Authorization Policy**, politika namenjena omejevanju dostopa na končne točke integracijskega API-ja na podlagi uporabniških vlog.
- **Basic Authentication Policy**, politika namenjena izvajanju HTTP Basic avtentikacije. Avtentikacija uporabnika se izvaja z integracijo z LDAP.
- **IP Whitelist Policy**, politika namenjena definiranju seznama IP-jev, s katerih so dovoljeni klici na integracijski API.
- **Rate Limiting Policy**, politika namenjena omejevanju števila klicev na časovno enoto.
- **WS Security Policy**, politika namenjena izvajanju avtentikacije na osnovi Web Service Security Username Token.
- **Keycloak OAuth Policy**, politika namenjena izvajanju avtentikacije na osnovi dostopnega žetona.

Poleg politik dostopa API prehod izvaja tudi tehnično[1] beleženje API klicev v dokumentno shrambo Elasticsearch. Metrike dostopa je mogoče spremljati preko portala KumuluzIntegration na nivoju integracijskega API-ja ali na nivoju organizacije.

Komponenta API Prehod se izvaja neodvisno od KumuluzIntegration platforme. V okviru integracijske platforme je mogoče namestiti več instanc API Prehodov. Priporočena je nastavitev v visoko-razpoložljivi konfiguraciji.

III Popis uporabljenih tehnologij in/ali morebitne dodatne opreme

Platforma KumuluzIntegration je sestavljena iz več komponent, ki temeljijo na različnih tehnologijah.

Osrednje komponente platforme KumuluzIntegration in uporabljene tehnologije:

[1] To pomeni, da ne izvaja vsebinskega beleženja, s čimer je mišljeno, da ne beleži t. i. payloada sporočil (v katerih so lahko recimo občutljivi podatki).

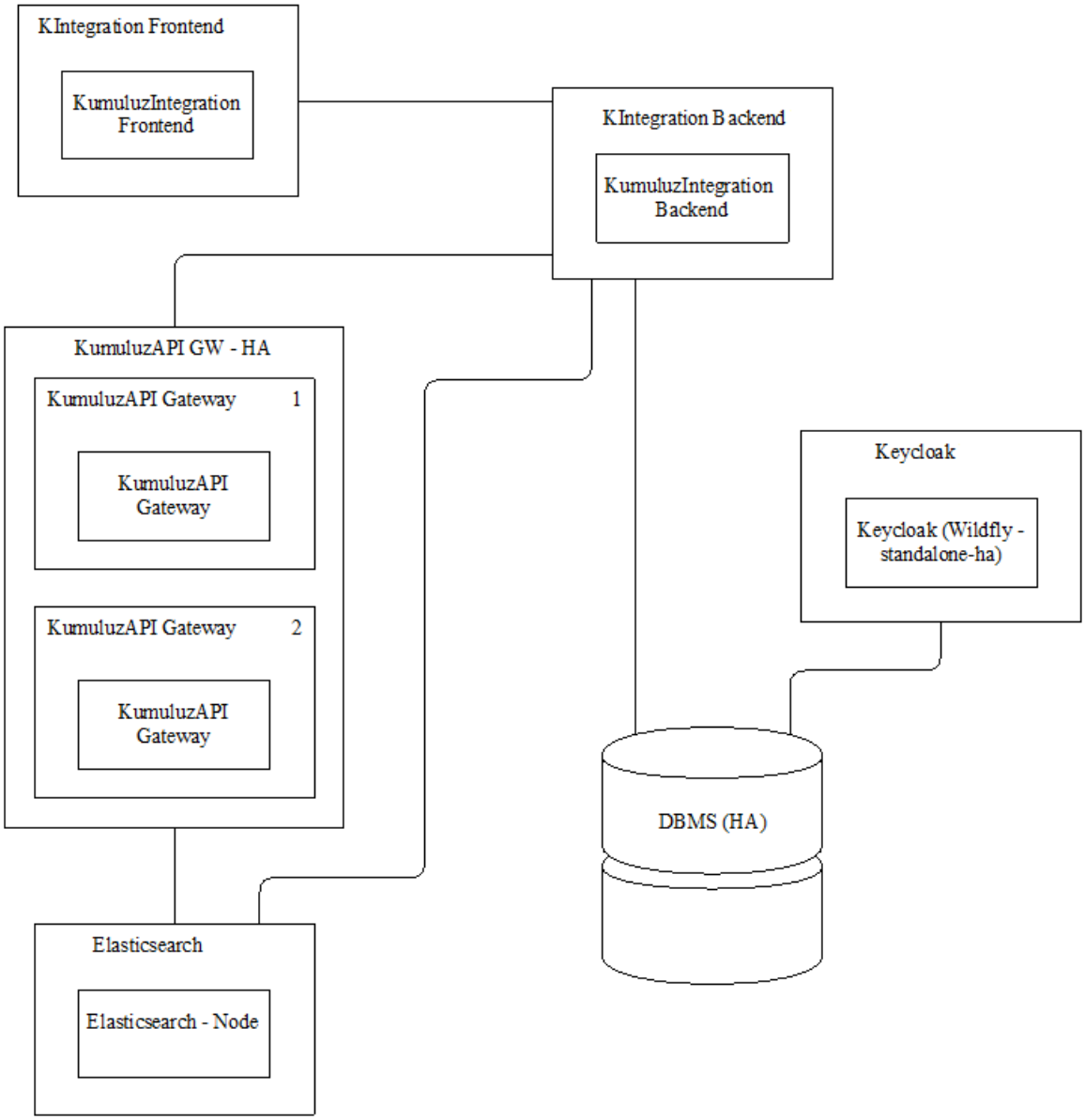
- KumuluzIntegration frontend: uporabniški vmesnik, implementiran kot spletna aplikacija (AngularJS).
- KumuluzIntegration backend: zaledna aplikacija, ki implementira poslovno logiko (Java – KumuluzEE Microservice Architecture).
- Kumuluz API Prehod (GW): API prehod, ki izvaja poslovno logiko posredovanja klicev na zaledne integracijske API-je (Java microservice).
- Keycloak: avtorizacijski strežnik za upravljanje uporabnikov platforme KumuluzIntegration (Wildfly).
- Elasticsearch: distribuirana dokumentna (NoSQL) podatkovna shramba s podporo za »full-text« iskanje. Podatkovna shramba se uporablja za konfiguracijo API prehodov in za shranjevanje metrik dostopa do integracijskih API-jev.
- Podatkovna shramba: Oracle podatkovna shramba KumuluzIntegration platforme.

Poleg osrednjih komponent KumuluzIntegration platforma lahko uporablja tudi nekaj opcijskih podpornih komponent, kot so:

- ELK stack: Elasticsearch, Logstach in Kibana, ki se lahko uporabi kot komponenta za centralno zbiranje logov komponent KumuluzIntegration in integracijskih API-jev. Integracijska platforma KumuluzIntegration se integrira z ELK stack instanco in iz nje pridobiva in prikazuje loge.
- ETCD gruča: ETCD gruča je distribuirana shramba ključ-vrednost, ki se uporablja za shranjevanje konfiguracij API-jev in komponent. ETCD gruča je integrirana z KumuluzIntegration platformo, preko katere lahko vnašamo in upravljamo konfiguracije API-jev.
- Docker, Kubernetes in Prometheus za elastično izvajanje integracijskih mikrostoritev z uporabo vsebnikov Docker, njihovo orkestracijo in spremljanje metrik izvajanja.

IV Arhitektura sistema

Naslednja slika 2 prikazuje arhitekturo sistema KumuluzIntegration in prikazuje komponente, njihove povezave, uporabo strežnikov in način postavitve rešitve v visoko razpoložljivo (HA – High Avaliability) konfiguracijo.



Slika 2 - KumuluzIntegration arhitektura HA postavitve

Integracijska platforma KumuluzIntegration povezuje več komponent in tehnologij. Postavitvena arhitektura predvideva namestitev platforme v visoko-razpoložljivi konfiguraciji, kar pomeni, da so vse komponente podvojene s čimer zagotovimo odpornost na izpad.

Namestitvena arhitektura predvideva izvajanje na platformi Linux. Visoko razpoložljivost dosežemo z uporabo standardnega mehanizma keepalived, ki bazira na protokolu VRRP. Mehanizem omogoča, da storitev keepalived namestimo na vseh vozliščih, kjer vsakemu vozlišču dodelimo prioriteto. Vozlišče z najvišjo prioriteto prevzame vIP naslov. V primeru, da pride do izpada vozlišča, vIP prevzame naslednje vozlišče (glede na prioriteto).

V Varnostni in zaščitni mehanizmi

Integracijska platforma KumuluzIntegration vključuje standardne mehanizme za zagotavljanje varnosti. Varnost je zagotovljena na več nivojih: KumuluzIntegration portal, API Prehod in na zalednih integracijskih API-ji.

Osrednja komponenta platforme je portal, preko katerega nadziramo in upravljamo integracije in integracijske API-je. Avtentikacija uporabnikov na spletnem portalu bazira na protokolu OpenID Connect (avtentikacijski nivo nad protokolom OAuth 2.0). Vsi viri zaledne REST storitve so zaščiteni, kar pomeni, da mora odjemalna aplikacija (portal, ki se izvaja v brskalniku) za dostop do virov pridobiti veljaven dostopni žeton. Avtentikacijo uporabnika in izdajo žetona izvaja avtorizacijski strežnik (Keycloak). Vsa komunikacija med komponentami KumuluzIntegration: frontend, backend, Keycloak in API Gateway poteka preko HTTPS (TLS).

Dostop odjemalnih aplikacij do integracijskih API-jev vedno poteka preko centralne točke API Prehod-a. API Prehod je namenjen izvajanju in nadzoru dostopov do zalednih API-jev. API Prehod podpira varnostne politike, s katerimi lahko zagotovimo in upravljamo varnost vseh API-jev na eni točki – preko KumuluzIntegration. Varnostne politike so v tem dokumentu že bile predstavljene (poglavje II.b API Prehod).

API Prehod lahko predstavlja le prvi nivo zaščite pri dostopu do zalednih integracijskih API-jev. Integracijska platforma omogoča implementacijo varnostnih mehanizmov tudi na nivoju zalednih API-jev. Pri uporabi API Prehodov lahko zaledne integracijske API-je izoliramo, saj lahko zagotovimo, da odjemalne aplikacije do njih dostopajo le preko API Prehod-a/ov.

Vsa komunikacija med odjemalnimi aplikacijami, API Prehod-i in zalednimi API-ji poteka preko HTTPS (TLS).