



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA FINANCE

URAD REPUBLIKE SLOVENIJE
ZA NADZOR PRORAČUNA

»Vzdrževanje in prilagoditve aplikativne programske opreme e- Notranja revizija«

TEHNIČNE SPECIFIKACIJE

Vsebina

1	Uvod	3
2	Predmet naročila	4
2.1	Osnovno vzdrževanje.....	4
2.1.1	Odzivni čas in čas reševanja.....	4
2.2	Podpora naročniku	5
2.3	Računalniške storitve v povezavi s prilagoditvami	6
2.4	Prilagoditve aplikativne programske opreme, vključno s pripravo navodil za nove/spremenjene/optimizirane funkcionalnosti	6
2.4.1	Predvidena vsebina prilagoditev	6
2.4.2	Priprava uporabniških navodil za nove/spremenjene/optimizirane funkcionalnosti.....	7
3	Opis obstoječega sistema	8
3.1	Splošni opis.....	8
3.2	Tehnološka zasnova	8
3.2.1	Arhitekturna shema aplikacije eNR	9
3.2.2	IIS FE-POSLOVNI – predstavitveni del poslovne aplikacije.....	9
3.2.3	IIS BE-POSLOVNI – zaledni del poslovne aplikacije	9
3.2.4	IIS FE-ADMIN – predstavitveni del administracijske aplikacije	10
3.2.5	IIS BE-ADMIN – zaledni del administracijske aplikacije	10
3.2.6	Izdelava in poganjanje izpisov in poročil	10
3.2.7	Hranjenje datotek in generiranih poročil v elektronski obliki.....	10
3.2.8	Namestitev aplikacije ter podatkovne baze	10
3.2.9	Tehnološka okolja	11
3.2.10	Karakteristike strežnikov.....	11
3.2.11	Specifikacija XML struktur	12
3.2.12	Specifikacije spletnih storitev.....	12
3.2.13	Varnostni in zaščitni mehanizmi	12
3.2.14	Integracije z zunanjimi sistemi.....	13
4	Splošne zahteve pri izvajanju storitev.....	14
4.1	Organizacija izvajanja storitev.....	14
4.2	Podpora končnim upravnikom	14
4.3	Generične tehnološke zahteve (GTZ)	14
4.4	Metodologija prilagoditev aplikacijske programske opreme.....	14
4.5	Proces RTP.....	15
4.5.1	Testiranje.....	15
4.6	Dokumentacija	16
4.7	Licence in izvorna koda.....	16
5	Viri	17

Kazalo slik

Slika 1: Aplikacijski nivoji – logična shema.....	8
Slika 2: Arhitektura aplikacije	9

Kazalo tabel

Tabela 1: Resnost problemov in odzivni čas ter čas, v katerem mora izvajalec odpraviti napako	5
Tabela 2: Karakteristike posameznih strežnikov:	11

Kratice

API	Vmesnik za namensko programiranje
ASP.NET	Microsoft tehnologija s pomočjo katere izdelujemo spletne strani
BE	Back-end – zaledni del aplikacije
CEH	Centralna elektronska hramba https://podatki.gov.si/dataset/centralna-elektronska-hramba-ceh-evem
DB	Database (podatkovna baza)
DMZ	Demilitarizirana cona
DRO	Državni računalniški oblak
DTO	Data Transfer Object – objekt, ki prenaša podatke med procesi (npr. request DTO posreduje vhodne podatke za proces, response DTO pa vrača podatke rezultatov nekega procesa) https://en.wikipedia.org/wiki/Data_transfer_object
FE	Front-end – predstaviteni del aplikacije
GDPR	<i>General Data-Protection Regulation</i>
GTZ	Generične tehnološke zahteve
HKOM	Hitro komunikacijsko omrežje
IIS	Internet Information Server – Microsoftov spletni aplikacijski strežnik
KDP	Kvalificirano digitalno potrdilo
MJU	Ministrstvo za javno upravo
PID	Projekt izvedenih del
PZI	Projekt za izvedbo
SaaS	Programska oprema kot storitev
SiCAS	Centralni avtentikacijski sistem (skupni gradnik)
SIPASS	Enotna točka za preverjanje identitete različnih uporabnikov
SOAP	Spletna storitev za komunikacijo med odjemalcem in strežnikom v skupnem jeziku XML
SSL	Kriptografski protokol, ki omogoča varno komunikacijo na medmrežju
SVN	Repozitorij izvirne kode in dokumentacije
TLS	Način šifriranja spletnega prometa
UAT	User Acceptance Testing

1 Uvod

Aplikacija e-Notranja revizija (eNR) je bila razvita z namenom vzpostavitve enotne informacijske podpore notranjemu revidiranju proračunskih uporabnikov. Z uvedbo aplikacije eNR se je izvajalcem notranjega revidiranja proračunskih uporabnikov ter Uradu RS za nadzor proračuna zagotovil temelj za uporabo enotne notranjerevizijske metodologije, podlag za učinkovito medsebojno komuniciranje in za sprotno zagotavljanje potrebnih informacij. Izvajalci notranjega revidiranja proračunskih uporabnikov ter Urad RS za nadzor proračuna kot centralni organ za harmonizacijo in koordinacijo notranjega revidiranja proračunskih uporabnikov so v aplikaciji vključeni v enoten sistem, s čimer je zagotovljena podlaga za pridobivanje sprotnih, objektivnih in potrebnih podatkov za usklajeno delovanje sistema notranjega nadzora javnih financ pri proračunskih uporabnikih. Aplikacija eNR je nameščena na infrastrukturo državnega računalniškega oblaka (DRO) Ministrstva za javno upravo in vsebuje devet vsebinskih modulov, integriranih v povezan sistem. Vsak vsebinski modul podpira predpisane procese in postopke, ki jih morajo v skladu z aktualnimi Usmeritvami za državno notranje revidiranje izvajati izvajalci notranjega revidiranja proračunskih uporabnikov. Zagotovljen je tudi elektronski arhiv vseh dokumentov. Administracija aplikacije je urejena v posebnem modulu, ki je nameščen kot ločena aplikacija (FE-Admin kot FrontEnd Administracija) in je dosegljiv samo iz HKOM omrežja, vstop v FE-Admin aplikacijo pa je omogočen le izbranim vlogam.

Avtentikacija uporabnikov je izvedena preko storitve SiCas z uporabo kvalificiranih digitalnih potrdil, avtorizacija pa je izvedena glede na dodeljeno vlogo uporabnika in pravice posameznih vlog, določenih v aplikaciji.

Aplikacija eNR je v produkcijskem delovanju, uporabljajo jo zaposleni v notranjerevizijskih službah proračunskih uporabnikov, Uradu RS za nadzor proračuna ter zunanji izvajalci storitev notranjega revidiranja (uporabniki znotraj HKOM in zunaj HKOM omrežja). Aplikacija je povezana z nekaterimi horizontalnimi gradniki (kot npr. Pladenj, CEH) v skladu s Smernicami za razvoj informacijskih storitev, izdanih s strani Ministrstva za javno upravo.

Aplikacija eNR je v trenutni verziji zgrajena v skladu z zahtevanimi postopki in procesi, kot jih za izvajalce notranjega revidiranja predpisujejo aktualne zakonske in podzakonske podlage s področja notranjega nadzora javnih financ. Prilagoditve morajo ohraniti obstoječe funkcionalnosti in povezljivosti s horizontalnimi gradniki, ter na podlagi zahtev naročnika omogočiti optimiziranje oz. izgradnjo dodatno zahtevanih funkcionalnosti aplikacije.

2 Predmet naročila

Predmet javnega naročila so storitve razvoja in vzdrževanja aplikativne programske opreme ter na podlagi storitev razvoja priprava navodil za nove funkcionalnosti.. Storitve so razdeljene glede na njihovo naravo ter glede na način njihovega naročanja in obračunavanja:

1. Osnovno vzdrževanje;
2. Podpora naročniku;
3. Računalniške storitve v povezavi s prilagoditvami;
4. Prilagoditve, vključno s pripravo navodil za nove/spremenjene/optimizirane funkcionalnosti.

2.1 Osnovno vzdrževanje

Osnovno vzdrževanje aplikativne programske opreme je vezano neposredno na aplikacijo oz. programsko kodo, storitve pa se izvajajo v okviru obstoječih funkcionalnosti sistema. Podrobnejši opis predvidenih storitev osnovnega vzdrževanja:

- zagotavljanje ustrezne razpoložljivosti, odzivnosti in usposobljenosti sodelujočih kadrov;
- vzpostavitev in vzdrževanje razvojnega okolja, stroški povezav v omrežje HKOM (izvajalec mora zagotoviti dostop do HKOM¹ na svoje stroške), uporaba sistema SVN;
- izvajanje administrativnih in skrbniških nalog, povezanih z izvajanjem pogodbe;
- vzdrževanje kode in dokumentacije sistema (tehnične in uporabniške);
- redno preverjanje pravilnosti in optimalnosti delovanja sistema preko dnevniških datotek in standardnih orodij ter obveščanje naročnika v primeru zaznanih posebnosti.

Storitve osnovnega vzdrževanja sistema začne izvajalec izvajati takoj po podpisu pogodbe.

2.1.1 Odzivni čas in čas reševanja

Zahtevke za odpravo napak lahko izvajalcu posreduje le skrbnik pogodbe, oziroma od njega pooblaščen oseba. Zahtevki se izvajalcu posredujejo po e-pošti.

Odzivni čas je čas, ki preteče od trenutka, ko skrbnik pogodbe ali od njega pooblaščen oseba izvajalcu pošlje zahtevek za odpravo napake, do trenutka, ko izvajalec na zahtevek odgovori in prične z reševanjem napake. Maksimalni odzivni čas je odvisen od prioritete zahtevka, kot ga v prijavi navede skrbnik pogodbe ali od njega pooblaščen oseba in po potrebi uskladi z izvajalcem.

Čas, v katerem mora izvajalec odpraviti napako, začne teči od začetka reševanja problema s strani izvajalca. Resnost problemov in odzivni čas ter čas, v katerem mora izvajalec odpraviti napako, so določeni v Tabeli 1.

¹ Cenik dostopa do HKOM omrežja se nahaja na tej povezavi: <https://www.gov.si/zbirke/storitve/vloga-in-navodila-za-oddaljeni-dostop/>

Tabela 1: Resnost problemov in odzivni čas ter čas, v katerem mora izvajalec odpraviti napako

Resnost problema	Maksimalni odzivni čas	Čas za odpravo napake	Primer
Kritična	2 uri*	4 ure* ²	Sistem ne deluje
Visoka	4 ure*	8 ur*	Sistem deluje deloma, ogrožene so nekatere pomembne funkcionalnosti
Pomembna	8 ur*	16 ur*	Sistem deluje deloma, ogrožene so le nekatere manj bistvene funkcionalnosti

* Šteje se, da ure tečejo znotraj delovnega časa, med 8. in 16. uro.

Če izvajalec oceni, da je napaka takšna, da je ne bo mogoče odpraviti v času, zahtevanem v tej točki, to nemudoma (v vsakem primeru pa v času, ki je določen za odpravo napake) pisno sporoči naročniku, z obrazložitvijo ter predlogom, v kolikšnem času je napako možno odpraviti. Naročnik izvajalcu predlog pisno potrdi ali zavrne. Če naročnik predlog zavrne, mora navesti obrazložitev zavrnitve.

V prijavi težave oziroma zahtevka za pomoč naročnik praviloma navede naslednje podatke:

- ime in priimek kontaktne osebe oziroma prijavitelja,
- naziv in naslov naročnika,
- oznako pogodbe o vzdrževanju oziroma drugo prepoznavno oznako, ki jo določi izvajalec,
- datum in čas prijave,
- kratek opis težave (razpoznavno ime težave),
- vrsta težave (opis težave, opredelitev vprašanja, programska napaka, napaka v dokumentaciji, drugo),
- resnost težave,
- predlagana prioriteta reševanja težave (visoka, srednja, nizka),
- podroben opis težave (ali posnetek ekrana v elektronski obliki),
- lastnosti delovnega okolja (vrsta in verzija operacijskega sistema, spletnega brskalnika...),
- ponovljivost težave (opis zaporedja ukazov oziroma okoliščin, pri katerih pride do težave),
- obstoj pomožne rešitve in, če obstaja, njen opis.

Kot eno reševanje težave se smatra vsako posamezno vprašanje oziroma težava, ki predstavlja funkcionalno zaključeno celoto.

Naročnik in izvajalec se lahko na sestanku dogovorita tudi za drugačen način in obliko prijave težave oziroma za drugačen način izmenjave informacij. Drugačen način in oblika prijave težave morata biti dokumentirana in parafirana s strani naročnika in izvajalca.

2.2 Podpora naročniku

Podpora naročniku zajema aktivnosti, ki pomenijo vzdrževanje pravilnega delovanja obstoječih funkcionalnosti sistema, vendar jih naročnik posebej naroča.

Podrobnejši opis predvidenih storitev podpore naročniku:

- sodelovanje z naročnikom in sistemsko službo ter z drugimi poslovnimi partnerji naročnika v primeru medsebojno povezanih in odvisnih sistemov;

² Pri kritični prioriteti zahtevka mora izvajalec začeti z reševanjem takoj, oziroma takoj, ko je to mogoče (npr. potreben predhoden poseg drugega izvajalca).

- odprava motenj pri delovanju in uporabi aplikativne programske opreme (diagnostika, reševanje, koordinacija in obveščanje), izredni tehnični posegi na sistemu, aplikacijah in podatkovnih zbirkah, glede na zahteve naročnika;
- pomoč pri dostopu do informacij o uporabi sistema, za katere so potrebne zahtevnejše poizvedbe po sistemu;
- priprava statističnih in analitičnih izdelkov.

Storitve Podpore naročniku začne izvajalec izvajati takoj po podpisu pogodbe.

2.3 Računalniške storitve v povezavi s prilagoditvami

Računalniške storitve v povezavi s prilagoditvami so storitve, ki so vsebinsko podobne storitvam podpore naročniku, vendar se vedno izvajajo v povezavi oziroma v obdobju pred in ob namestitvi posodobitev programske opreme. Obsegajo:

- preverjanje delovanja na ciljnih tehnologijah in okoljih, preučevanje tehnoloških novosti, povezanih z vzdrževano programsko opremo ter priprava predlogov in ukrepov za izboljšanje zanesljivosti ter optimalnosti njenega delovanja;
- komunikacija in usklajevanje z naročnikom, upravitelji infrastrukture in uporabniki, glede možnih prilagoditev oz. optimizacij vzdrževane programske opreme;
- sodelovanje pri analizi in pripravi podrobnih tehničnih implementacijskih specifikacij uporabniških zahtev za dodajanje novih in izboljšanje obstoječih funkcionalnosti programske opreme;
- druge računalniške storitve v povezavi s prilagoditvami aplikacije.

2.4 Prilagoditve aplikativne programske opreme, vključno s pripravo navodil za nove/spremenjene/optimizirane funkcionalnosti

Prilagoditve aplikativne programske opreme zajemajo storitve, ki spreminjajo oz. optimizirajo funkcionalnosti aplikativne programske opreme. Prilagoditve morajo ohraniti obstoječe funkcionalnosti in povezljivosti s horizontalnimi gradniki, ter na podlagi zahtev naročnika omogočiti optimiziranje oz. izgradnjo dodatno zahtevanih funkcionalnosti aplikacije.

Podrobnejši opis predvidenih storitev:

- Prilagajanje, dograjevanje in optimiziranje funkcionalnosti aplikativne programske opreme ter izboljševanje njenih lastnosti delovanja in uporabnosti glede na vsebinske in tehnične zahteve naročnika;
- prilagajanje aplikativne programske opreme glede na spremembe systemskega okolja in operacijskega sistema ter glede na potrebe ostalih povezanih informacijskih sistemov;
- različne spremembe na aplikativni programski opremi, preko uporabniškega vmesnika ali s posebnimi orodji, prilagoditve, nastavitve, parametrizacija, spremembe konfiguracije, posegi na podatkovni zbirki, migracije podatkov;
- priprava in posodabljanje uporabniških navodil za nove/spremenjene/optimizirane funkcionalnosti.

2.4.1 Predvidena vsebina prilagoditev

Vsebina - funkcionalnosti prilagoditev bodo določene za vsako prilagoditev posebej, saj v trenutku naročila potrebe po novih/spremenjenih/optimiziranih funkcionalnosti še niso znane.

Ostala predvidena področja prilagoditev:

- izboljšanje funkcionalnosti orodij za načrtovanje, izvajanje, poročanje notranje revizije ter spremljanja njenih učinkov,

- izboljšanje uporabniškega vmesnika,
- nove in izboljšane komponente obrazcev,
- dodatni procesni koraki in njihove kombinacije,
- izboljšana dostopnost sistema za uporabnike.

2.4.2 Priprava uporabniških navodil za nove/spremenjene/optimizirane funkcionalnosti

Priprava uporabniških navodil za nove/spremenjene/optimizirane funkcionalnosti zajema dopolnitev in posodobitev obstoječih uporabniških navodil za nove oz. izboljšane funkcionalnosti aplikacije.

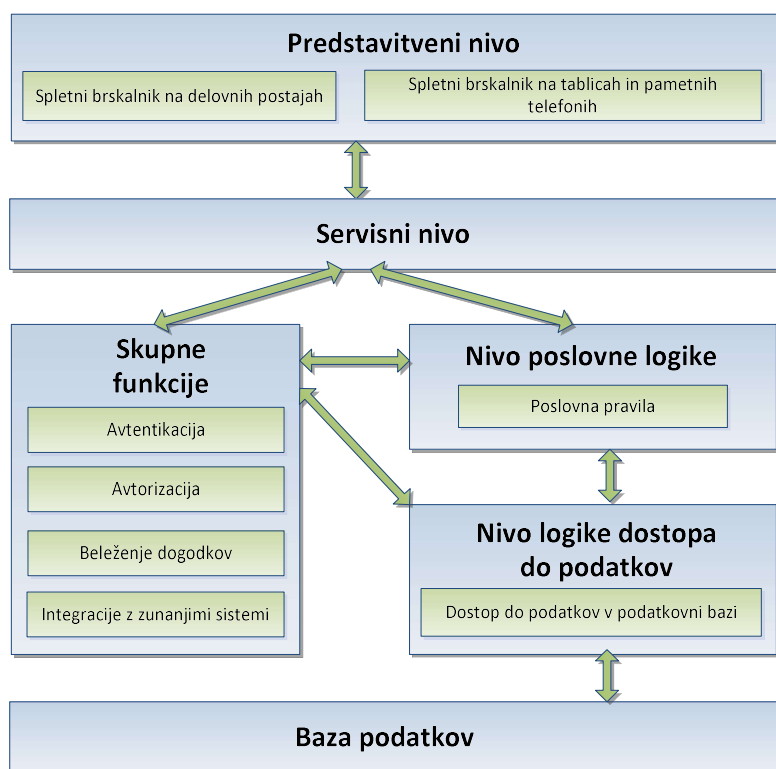
3 Opis obstoječega sistema

3.1 Splošni opis

eNR je informacijska rešitev, namenjena podpori delovanja izvajalcev notranjega revidiranja in Urada RS za nadzor proračuna kot centralnega organa za razvoj, koordinacijo in preverjanje delovanje sistema notranjega nadzora javnih financ. Aplikacija ima modularno zasnovo, vsi moduli pa so integrirani v povezan sistem, v katerem je optimiziran avtomatski prenos podatkov. Modularni sistem ima opredeljene API vmesnike med posameznimi sloji aplikacijskih gradnikov, kjer je poslovne funkcije mogoče klicati preko ReST arhitekturnega modela. Storitve kot taka je uporabnikom ponujena po t.i. SaaS (Software as a Service) modelu, tako da pri uporabnikih ni potreben noben poseg v infrastrukturo, potrebujejo samo internetno povezavo ter spletni brskalnik. Avtentikacija uporabnikov je izvedena preko SiCas z uporabo kvalificiranih digitalnih potrdil, avtorizacija pa je v aplikaciji izvedena glede na vlogo posameznega uporabnika ter pravice vlog.

Aplikacija je zasnovana večnivojsko. Sestavljena je iz predstavitvenega nivoja, ki je izdelan kot samostojna aplikacija in servisnega nivoja, ki je izdelan kot zaledna aplikacija in vsebuje dodatne sloje za poslovno logiko, dostop do podatkov in skupne funkcije.

Slika 1: Aplikacijski nivoji – logična shema



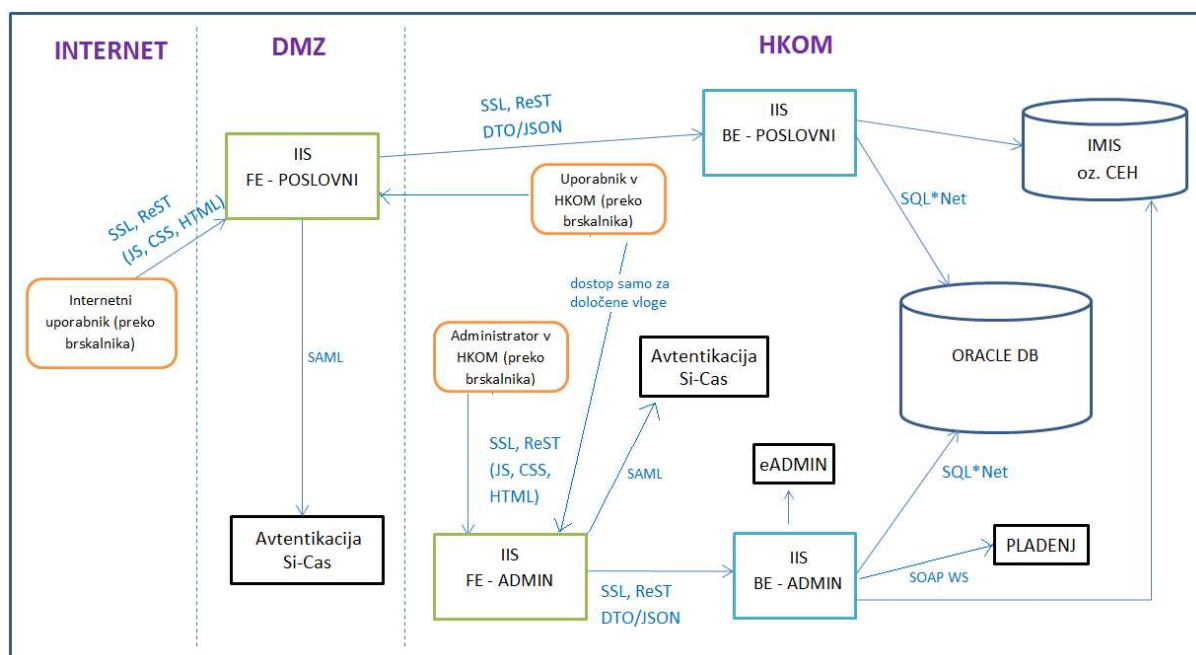
3.2 Tehnološka zasnova

Glavne značilnosti tehnološke zasnove so:

- uporaba obstoječih horizontalnih gradnikov,
- integracije prek spletnih storitev ("web services"),
- modularnost sistema.

3.2.1 Arhitekturna shema aplikacije eNR

Slika 2: Arhitektura aplikacije



3.2.2 IIS FE-POSLOVNI – predstavitveni del poslovne aplikacije

To je predstavitvena (front-end) IIS aplikacija v DMZ segmentu. Aplikacija vsebuje poslovne module in je namenjena tako internetnim kot HKOM uporabnikom. Uporabniki dostopajo do aplikacije s HTML5 kompatibilnim brskalnikom in kvalificiranim digitalnim potrdilom. Aplikacija dovoli dostop le ustrezno avtenticiranim ter avtoriziranim uporabnikom. Osnovna avtentikacija se izvede s pomočjo Si-Cas oziroma Si-Pass storitev, avtorizacija uporabnika (njegove vloge glede na notranjerevizijsko službo) pa se izvede znotraj aplikacije.

Komunikacija od odjemalca do IIS poteka preko SSL varne povezave, ki se zaključi na IIS-u z uporabo KDP.

Uporabniški del poslovne aplikacije je izdelan kot ASP.NET spletna aplikacija in teče na IIS strežniku v DMZ segmentu. ASP.NET aplikacija na strežniku pripravi začetno ogrodje strani. Od tu naprej pa se s pomočjo JavaScript kode aplikacija izvaja v brskalniku odjemalca kot SPA (Single Page Application). Komunikacija z zalednim delom (BE – POSLOVNI) poteka preko ReST klicev, vhodni in izhodni podatki se prenašajo kot DTO objekti.

Komunikacija med odjemalcem in IIS strežnikom poteka po HTTPS protokolu z uporabo kvalificiranih digitalnih potrdil.

3.2.3 IIS BE-POSLOVNI – zaledni del poslovne aplikacije

To je zaledni (back-end) del poslovne IIS aplikacije v HKOM omrežju, ki sprejema zahteve od predstavitvenega dela aplikacije. Zahtevki prihajajo po REST modelu in HTTPS protokolu. V avtentikacijskem headerju so informacije o uporabniku in geslu, s katerim se preverja, da je zahtevek nedvomno prišel od predstavitvenega sloja aplikacije (nastavitve so shranjene v šifrirani obliki v konfiguracijski datoteki aplikacijskega strežnika na predstavitvenem delu).

Vhodno – izhodni podatki so v obliki DTO in vsebujejo samo tiste podatke, ki so za posamezno operacijo potrebni. Uporabnik nikoli ne dobi podatke neposredno iz tabele v bazi, saj poteka to vedno preko nadzorovane operacije polnjenja podatkov v izhodni DTO.

IIS BE – POSLOVNI se na bazo prijavi z baznim uporabnikom, ki ima minimalni nabor pravic samo na tabelah, s katerimi aplikacija dela.

3.2.4 IIS FE-ADMIN – predstavitveni del administracijske aplikacije

To je predstavitvena (front-end) IIS aplikacija v HKOM segmentu, ki je namenjena samo za administracijo aplikacije. Uporabljajo jo administratorji aplikacije na strani naročnika.

Sicer pa veljajo zanjo enake tehnične specifikacije, kot za IIS FE – POSLOVNI.

3.2.5 IIS BE-ADMIN – zaledni del administracijske aplikacije

To je zaledna (back-end) IIS aplikacija v HKOM omrežju, ki obdeluje zahteve predstavljene Admin aplikacije. Aplikacijski uporabnik na bazi ima minimalni nabor pravic samo na objektih, ki so potrebni za administracijo aplikacije.

Sicer pa veljajo enake tehnične specifikacije kot za IIS BE – POSLOVNI.

3.2.6 Izdelava in poganjanje izpisov in poročil

Specifika aplikacije je veliko število različnih vrst nestandardiziranih poročil v DOCX formatu, pri čemer ne gre za statistične izpise.

Poročila se kreirajo z uporabo orodja Docentric (<https://www.docentric.com/>). To orodje omogoča uporabo predlog, ki se pripravijo v Microsoft Word obliki z dodatkom uporabe določenih podatkovnih struktur. Predloge se lahko pripravijo na osebem računalniku, ki ima nameščen Microsoft Word ter ustrezno Docentric orodje za urejanje predlog. Tako pripravljene predloge se uporabljajo v aplikaciji, pri čemer aplikacija uporabi predlogo in v omenjene podatkovne strukture v predlogi dinamično napolni vsebinske podatke. Za uporabo Docentric orodja za polnjenje predlog znotraj zalednega dela aplikacije ni potrebna uporaba ali nakup licence. Licenca je potrebna samo za pripravo predlog. V primeru aplikacije eNR izvajalec pripravi vse predloge in jih namesti v aplikacijo ob instalaciji aplikacije. Izvajalec potrebuje Developer OEM License (<https://www.docentric.com/purchase/license-types>), ki mu omogoča kreiranje predlog ter uporabo in namestitvev Docentric orodja za namene zunanjih aplikacij brez dodatnih stroškov za ponudnika storitve produkcijskega oziroma testnega okolja v DRO (MJU) in uporabnike aplikacije. Izvajalec skrbi za vse kasnejše spremembe predlog v skladu s predhodnim naročilom naročnika. S strani skrbnika okolja (MJU) in končnih uporabnikov aplikacije zato v zvezi z uporabo Docentric ni potreben nakup kakršnekoli licence.

3.2.7 Hranjenje datotek in generiranih poročil v elektronski obliki

Proces notranjega revidiranja vsebuje veliko število različnih dokaznih gradiv, ki jih je treba hraniti. V aplikaciji bo mogoče dodajati datoteke, ki so nastale izven aplikacije (Word, Excel, PDF skenirani dokumenti, ...) ter dokumente, ki jih aplikacija generira (večinoma DOCX). Potrjene končne verzije dokumentov se hranijo v CEH.

Fizično je del teh dokumentov hranjen v podatkovni bazi, del v CEH. Zaledni del aplikacije omogoča potrebne mehanizme za integracijo s CEH.

3.2.8 Namestitvev aplikacije ter podatkovne baze

Aplikacija in podatkovna baza sta nameščeni v državnem računalniškem oblaku (DRO) okolja MJU.

3.2.9 Tehnološka okolja

Aplikacija je pri naročniku nameščena v dveh tehnoloških okoljih:

- testno in
- produkcijsko.

Testno okolje je namenjeno testiranju novih različic rešitve in običajno "prehiteva" ostali okolji za eno ali več različic rešitve.

Produkcijsko okolje je namenjeno izvajanju storitev.

Dosegljivost okolij:

- Testno okolje je dosegljivo iz omrežij v omrežju HKOM.
- Izvedbeni del produkcijskega okolja je dosegljiv javno, razen administrativnega dela, ki je prav tako dosegljiv le iz omrežij v omrežju HKOM.

3.2.10 Karakteristike strežnikov

Vsi strežniki so nameščeni v virtualnem okolju. Naslednja tabela prikazuje karakteristike posameznih strežnikov:

Tabela 2: Karakteristike posameznih strežnikov:

Okolje	Naziv strežnika	Karakteristike
Produkcijsko okolje	IIS FE-POSLOVNI	32GB RAM, 8C, 160GB HD, Windows server 2019, IIS, .NET Framework
	IIS BE-POSLOVNI	32GB RAM, 12C, 250GB HD, Windows server 2019, IIS, .NET Framework
	IIS FE-ADMIN	32GB RAM, 8C, 160GB HD, Windows server 2019, IIS, .NET Framework
	IIS BE-ADMIN	32GB RAM, 12C, 250GB HD, Windows server 2019, IIS, .NET Framework
	Bazni strežnik (Obe BE aplikaciji uporabljata isti bazni strežnik ORACLE)	64GB RAM, 16C, 120GB HD. Ta strežnik je povezan na shared storage kjer so Oracle DB datoteke
Testno okolje	Vse na istem Virtualnem strežniku: IIS FE-POSLOVNI, IIS BE-POSLOVNI, IIS FE-ADMIN, IIS BE-ADMIN	32GB RAM, 12C, 300GB HD, Windows server 2019, IIS, .NET Framework
	Bazni strežnik (Obe BE aplikaciji uporabljata isti bazni strežnik ORACLE)	16GB RAM, 8C, 120GB HD Ta strežnik je povezan na shared storage kjer so Oracle DB datoteke.

3.2.11 Specifikacija XML struktur

Od XML struktur je uporabljena zgolj možnost izvoza podatkov v XML formatu, ki služi kot osnova za uporabo v generatorju poročil in izpisov.

Če se bo pokazala potreba, se bo v kasnejši fazi omogočalo uvoze nekaterih šifrantov preko predpisanih XML struktur, ki so specifični za vsako notranje-revizijsko službo posebej.

3.2.12 Specifikacije spletnih storitev

Zaledni del aplikacije je sestavljen iz dveh samostojnih delov:

- a) administrativnega dela s svojim API vmesnikom, ki se nahaja v varovanem HKOM segmentu;
- b) splošnega dela s svojim API vmesnikom, ki se nahaja v varovanem HKOM segmentu.

Predstavitveni del aplikacije je postavljen takole:

- a) uporabniki izven HKOM preko interneta dostopajo do spletnih strežnikov, ki so postavljeni v DMZ segmentu. Ti strežniki so preko požarne pregrade povezani s splošnim zalednim delom aplikacije;
- b) uporabniki znotraj HKOM-a dostopajo do spletnih strežnikov, ki so postavljeni v DMZ segmentu;
- c) administratorji aplikacije imajo v HKOM omrežju ločen spletni strežnik, ki dostopa do administrativnega zalednega dela aplikacije.

3.2.13 Varnostni in zaščitni mehanizmi

Avtentikacija vstopa v uporabniško aplikacijo: osnovna avtentikacija uporabnika se izvaja s pomočjo Si-Cas oziroma Si-Pass. Uporabnik, ki se ustrezno avtentificira, dobi vstop v uporabniško aplikacijo (front-end) na podlagi veljavnih vlog v aplikaciji.

Avtorizacija v uporabniški aplikaciji: avtenticiranemu uporabniku aplikacija preveri vloge in mu glede na to omogoči oz. skrije oz. onemogoči določene funkcionalnosti aplikacije. Uporabniški vmesnik prikazuje samo tisto, do česar ima uporabnik dostop in omogoči samo operacije, ki jih uporabnik sme izvajati.

Avtentikacija in avtorizacija na zalednem delu: klic na zaledni del je prav tako v REST obliki. V glavi zahtevka je tudi avtentikacijski žeton, v katerem je podatek o uporabniku in geslu, ki ga poda IIS strežnik predstavitvenega dela aplikacije. Na podlagi konfiguracije pravic uporabnika nato poslovna logika prejeti zahtevek avtentificira in ga izvede ali zavrne (razen če je dovoljen anonimen dostop do neke API metode, ko se izvedba zahtevka pošlje v izvajanje brez preverjanja).

Na zalednem delu sta dve aplikaciji. Ena je namenjena končnim uporabnikom, ki uporabljajo poln nabor funkcionalnosti (tipično so to notranjerevizijske službe, Urad za nadzor proračuna in deloma tudi zunanji izvajalci notranjega revidiranja). Druga pa je namenjena administratorjem aplikacije za administracijska opravila na aplikaciji ter izbranim uporabniškim vlogam (vodjem notranjerevizijskih služb), ki so odgovorne za urejanje ključnih vsebinskih matičnih podatkov (tipično podatkov o notranjerevizijski službi ter njim podrejenih proračunskih uporabnikih).

Na ta način je poskrbljeno za dodaten nivo varovanja podatkov tako nastavitvenih parametrov in šifrantov aplikacije kot ključnih vsebinskih matičnih entitet.

Beleženje dogodkov v aplikaciji: zaledna aplikacija beleži dogodke in jih zapisuje v datotečni sistem v skupno datoteko. Uvedena je periodična rotacija na dnevni ali tedenski bazi, odvisno od velikosti. Te beležke MJU na zahtevo posreduje naročniku, ki jih po potrebi posreduje izvajalcu, da lahko poišče vzroke napak in nepravilnosti v delovanju.

Beleženje na predstavitvenem nivoju poteka na nivoju sporočil na konzolo brskalnika.

3.2.14 Integracije z zunanjimi sistemi

Centralna hramba: hramba ključnih in potrjenih dokumentov, razen predlog izpisov, je v horizontalnem gradniku »Centralna hramba« MJU, ki zagotavlja skladno dolgoročno hrambo vseh digitalnih vsebin, časovne žige ter revizijsko sled. Primarna funkcija storitve centralne hrambe gradiva (CEH) je zagotovitev centralizirane, zakonsko skladne in certificirane hrambe dokumentarnega gradiva, ki izpolnjuje raznolike funkcionalne zahteve različnih informacijskih sistemov po hrambi gradiva na infrastrukturi, ki zagotavlja brezhibno in nemoteno delovanje ter varno hrambo podatkov.

Integracije med eNR in CEH je vzpostavljena preko namenskih spletnih servisov:

- prek spletnega vmesnika REST
- prek spletnega vmesnika SOAP

Promet med storitvijo in njenimi odjemalci je zaščiten s šifriranjem po protokolu TLS, ki je trenutno de-facto standard pri izbiri načina zaščite podatkov v fazi prenosa po omrežju.

Uvoz podatkov iz AJPES-a: Povezava z AJPES-om omogoča pridobitev in osveževanje podatkov o proračunskih uporabnikih ter o njihovih finančnih podatkih (višina proračuna oz. poraba v preteklem letu).

Integracija se izvaja na naslednji način: naročnik ima že utečen postopek, s katerim vsako leto pridobi podatke s strani AJPES v obliki standardizirane Excel datoteke s predefiniranim formatom. Administratorska aplikacija omogoča uvoz datoteke v aplikacijo ter obdelavo datoteke za pridobitev želenih podatkov. Uvoz se izvede enkrat letno predvidoma v mesecu marcu, ko so podatki na voljo s strani AJPES.

UJP preko storitve PLADENJ: pridobivanje podatkov o registru proračunskih uporabnikov se izvaja preko storitve PLADENJ, ki zagotavlja dostop do podatkov tega registra.

Varnostni podsistem: varnostni podsistem je del skupnega modula eNR in predstavlja osnovo za obvladovanje uporabnikov, skupin, organizacijskih enot in pravic, ki jih uporabniki imajo. Podsistem skrbi za avtentikacijo in avtorizacijo vseh uporabnikov aplikacije eNR.

Sporočilni sistem: aplikacija se povezuje s sporočilnim sistemom preko SMTP protokola.

4 Splošne zahteve pri izvajanju storitev

4.1 Organizacija izvajanja storitev

Prilagoditve aplikacije, vezane na pomembnejše spremembe pravnih in strokovnih podlag področja notranjega nadzora javnih financ, ki v večji meri vplivajo na funkcionalnosti posamičnih modulov aplikacije, se jo označi kot "pomembnejše".

Projektni vodja izvajalca mora za pomembnejše prilagoditve v skladu z vsakokratnim terminskim načrtom predložiti podroben načrt izvedbe naročenih storitev, ki mora vključevati:

- podroben seznam aktivnosti,
- predviden začetek in trajanje vsake aktivnosti,
- podatke o medsebojnih odvisnostih aktivnosti,
- predpogoje za izvedbo posamezne aktivnosti in
- načrt izdelkov.

Izvajalec mora načrt izvedbe z naročnikom redno usklajevati. Vsi usklajevalni in delovni sestanki med naročnikom in izvajalcem morajo biti dokumentirani v elektronski obliki, pri čemer mora zapisnike pripraviti izvajalec, naročnik pa jih potrdi.

Komuniciranje poteka v obliki elektronske pošte ali v obliki sestankov, ki se glede na temo in razmere izvedejo na lokaciji naročnika, na lokaciji izvajalca ali v obliki spletnega sestanka.

4.2 Podpora končnim uporabnikom

Podpora končnim uporabnikom rešitve je organizirana dvonivojsko:

1. nivo podpore - zagotavlja ga Enotni kontaktni center naročnika (EKC);

2. nivo podpore - ki se deli na:

- **vsebinsko** podporo in jo izvaja naročnik,
- **tehnično** podporo izvaja tehnična ekipa naročnika, ob pomoči izvajalca v okviru storitve 2.2 Podpora naročniku.

4.3 Generične tehnološke zahteve (GTZ)

Vse na novo razvite funkcionalnosti in prilagoditve morajo biti skladne z Generičnimi tehnološkimi zahtevami³ (v nadaljevanju: GTZ), pri vseh prilagoditvah oz. posegih v aplikativno programsko opremo pa je izvajalec dolžan upoštevati tudi Smernice za razvoj informacijskih rešitev⁴.

Če izvajalec opazi pomanjkljivosti na tehnološki infrastrukturi, na kateri bo delovala informacijska rešitev, mora nanje opozoriti naročnika in predlagati odpravo pomanjkljivosti.

4.4 Metodologija prilagoditev aplikacijske programske opreme

Naročnik podpira sodobne agilne pristope k prilagoditvam aplikacijske programske opreme, vendar je izbira metodologije prepuščena izvajalcu.

³ <https://nio.gov.si/nio/asset/dokument+genericne+tehnoloske+zahteve+gtz-743>

⁴ <https://nio.gov.si/nio/asset/smernice+mju+za+razvoj+informacijskih+resitev-768>

4.5 Proces RTP

Naročnik ima pri prilagoditvah in namestitvi posodobitev aplikacijske programske opreme vzpostavljen proces, imenovan "RTP" (Razvoj-Test-Produkcija), ki določa tipičen način vzpostavljanja informacijskih rešitev. Uporablja se za vsako prilagoditev aplikativne programske opreme.

Osnovna pravila procesa določajo prilagoditve programske opreme na **razvojnem** okolju izvajalca (pri tem je izvajalcu prepuščena možnost, da pri sebi po potrebi vzpostavi več okolij).

Ko je prilagoditev programske opreme izdelana in testirana v okolju izvajalca, jo le ta pripravi v obliki primerni za namestitev (programske kode, vse pripadajoče programske knjižnice, konfiguracijske datoteke in izvedbene skripte) in jo odloži v repozitorij programske kode. Po avtomatskem varnostnem testiranju programske kode, naročnikova sistemska služba zgradi in namesti programsko rešitev v **testno** okolje naročnika. Tu je na voljo za izvedbo uporabniškega sprejemljivostnega testiranja (UAT - "ang. *user acceptance test*") s strani naročnika v obsegu, ustreznem pomembnosti prilagoditve.

Ko je UAT uspešno zaključen, sledi namestitev v **produkcijsko** okolje. Ob pomembnejših prilagoditvah se po presoji naročnika lahko izvede tudi penetracijsko varnostno testiranje in/ali zmogljivostno testiranje. Zadnja testa se izvajata pred namestitvijo v produkcijsko okolje, oziroma pred produkcijsko uporabo aplikativne programske opreme.

Uspešno opravljeno testiranje in naročniku v celoti predana dokumentacija sta predpogoj za prevzem posamezne prilagoditve, ki jo naročnik potrdi s podpisanim prevzemnim zapisnikom.

4.5.1 Testiranje

Testiranje informacijske rešitve je aktivnost, ki spremlja razvoj informacijske rešitve v vseh njegovih fazah. Namen testiranja je zagotoviti kvalitetno informacijsko rešitev, ki je robustna, skladna s tehničnimi in vsebinskimi specifikacijami, varna in odporna na obremenitve – bodisi zaradi velikega števila transakcij bodisi zaradi velikega števila uporabnikov.

V razvojnem okolju izvajalec izvaja "*unit*" teste, ki naj pokrivajo velik odstotek izvirne kode, ob prilagoditvah sistema pa mora izvesti tudi regresijsko testiranje, ki preveri vpliv nove kode na obstoječo. Izvede se tudi funkcionalno testiranje v skladu z zahtevami naročnika. Izvajalec sproti izvaja tudi varnostne in obremenilne teste.

Za avtomatsko varnostno testiranje lahko uporabi tudi naročnikovo okolje za odlaganje kode (repozitorij SVN), na katerem se vsaka odložena koda avtomatsko testira. Rezultati testiranja so glede na resnost ranljivosti razvrščeni v tri stopnje. Pogoj za nadaljevanje postopka nameščanja je koda brez varnostnih ranljivosti najvišje stopnje.

Uspešnemu avtomatskem varnostnemu testiranju sledi uporabniško funkcionalno testiranje (UAT), ki ga izvede naročnik. Za naročnika izvajalec pripravi načrt testiranja s seznamom testov, koraki izvajanja vsakega testa in pričakovanimi rezultati testa. Naročnik pri funkcionalnem testiranju ni omejen na načrt testiranja. S tem testiranjem naročnik ugotovi, da so izpolnjene vse njegove funkcionalne zahteve.

Po uspešnem funkcionalnem testiranju lahko naročnik izvede tudi penetracijsko testiranje ("ročno" varnostno testiranje s poskusi izkoriščanja varnostnih vrzeli celotnega sistema - ne le kode same).

Če naročnik po prilagoditvi aplikativne programske opreme predvideva večje število transakcij ali veliko število dodatnih uporabnikov sistema, lahko skupaj z izvajalcem izvede tudi obremenitveno ali celo stresno testiranje.

4.6 Dokumentacija

Naročnik zahteva natančno in ažurno dokumentiranje aplikativne programske opreme v slovenskem jeziku. Dokumentacija mora biti osvežena ob vsaki spremembi na aplikativni programski opremi oziroma ciljnih okoljih. Preda se na način, da se ob vsaki prilagoditvi odda vsa dokumentacija kumulativno in ne zgolj dokumentacija, ki je bila osvežena oz. dodana.

Poleg dokumentacije arhitekture in strukture sistema morajo biti osveževana tudi navodila za uporabo sistema glede na vlogo, ki jo ima posamezen uporabnik.

Izvajalec ves čas trajanja vzdrževanja sistema dopolnjuje uporabniška navodila v skladu s spremembami, ki so nastale v sistemu kot posledica prilagoditev in jih predaja naročniku, odloži pa jih tudi v repozitorij SVN. Uporabniška navodila morajo biti ločena glede na vlogo, ki jo ima posamezen uporabnik.

Vsa navodila morajo biti v elektronski obliki - v formatu, primernem za objavo na spletu (npr. dokumenti HTML, rtf, xls, pdf) in za uporabo v sistemu spletnega učenja, hkrati pa dosegljiva uporabnikom iz aplikativne programske opreme - glede na vlogo, s katero je trenutno prijavljen in glede na funkcionalnost, ki jo v sistemu trenutno opravlja.

Zahtevana dokumentacija:

- Tehnična dokumentacija sistema:
 - projekt za izvedbo (PZI),
 - primeri uporabe,
 - načrt testiranja,
 - projekt izvedenih del (PID)⁵,
 - morebitna druga dokumentacija za potrebe naročnika.
- Navodila za uporabo:
 - administratorski del v celoti,
 - poslovni del v celoti.

Izvajalec lahko oblikuje dodatno dokumentacijo, ki bo njemu in naročniku olajšala vzpostavitev in vzdrževanje sistema.

PZI naj bo zastavljen strukturirano - glede na arhitekturo tehnologije, PID pa naj to strukturo ohrani. Elementi PZI so določeni v dokumentu GTZ (GTZ-PROJEKT-PZI-*).

4.7 Licence in izvorna koda

Vsa izvorna koda sistema ob predaji sistema preide v last naročnika. Naročnik praviloma sam prevede kodo in zgradi sistem ("*build*"). Izvajalec v rešitvi ne sme uporabiti knjižnic, drugih delov kode ali artefaktov, ki ne bi mogli preiti v last naročnika (lastne rešitve ali "*third-party*" licence) in bi lahko povzročili težave pri avtonomnosti naročnika pri vzdrževanju in/ali nadaljnjem razvoju sistema. Naročnik dopušča uporabo odprtokodnih knjižnic, ki imajo aktivno podporo odprtokodne skupnosti.

⁵ Del PID izpolni tudi naročnikova sistemska služba (dokumentiranje nastavitvev, namestitve na konkretno strojno opremo in dokumentiranje nižjih nivojev programske opreme)

5 Viri

- GTZ - Generične tehnološke zahteve
(<https://nio.gov.si/nio/asset/dokument+genericne+tehnoloske+zahteve+gtz-743>)
- Smernice za razvoj informacijskih rešitev
(<https://nio.gov.si/nio/asset/smernice+mju+za+razvoj+informacijskih+resitev-768>)
- GDPR - General Data Protection Regulation
(<https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>)