



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA ZDRAVJE

Štefanova ulica 5, 1000 Ljubljana T: 01 478 60 01
F: 01 478 60 58
E: gp.mz@gov.si
www.mz.gov.si

e zdravje



Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski socialni sklad



»Vzdrževanje varnostne sheme«

Tehnične specifikacije



KAZALO VSEBINE

1. Predmet javnega naročila	3
2. Opis informacijske rešitve.....	3
2.1 VARNOSTNA SHEMA.....	3
3. Obseg javnega naročila	4
4. Tehnološke zahteve	6
5. Zahteve glede odzivnega časa	7
6. Nefunkcionalne zahteve.....	8
7. DRUGE ZAHTEVE	10

KAZALO TABEL

Tabela 1: Odzivni časi v primeru zahtevkov zaradi napak oz. motenj	7
Tabela 2: Določitev stopnje napake	8

SLOVAR

VS – Informacijska rešitev Varnostna shema
RIZDDZ – Register izvajalcev zdravstvene dejavnosti in delavcev v zdravstvu
RPPE – Register pacientov in prostorskih enot – spletni servis, ki deluje v eZdravju
ZZZS – Zavod za zdravstveno zavarovanje Slovenije
MJU – Ministrstvo za javno upravo
SSO – Mehanizem enotne prijave – Single Sign-On
WS – Spletna storitev (angl. Web Service)
zNET – Varno zdravstveno omrežje
SAML – Standard za izmenjavo avtentikacijskih in avtorizacijskih podatkov (angl. Security Assertion Markup Language)
OAUTH2 – Protokol za avtorizacijo
XACML – Razširljiv jezik za opisovanje kontrole dostopa (angl. eXtensible Access Control Markup Language)



1. PREDMET JAVNEGA NAROČILA

Predmet javnega naročila je:

- osnovno vzdrževanje informacijske rešitve Varnostna shema (VS)
- dopolnilno vzdrževanje informacijske rešitve Varnostna shema

2. OPIS INFORMACIJSKE REŠITVE

2.1 VARNOSTNA SCHEMA

Varnostna shema (VS) je centralna varnostna shema eZdravja. Informacijska rešitev Varnostne sheme je kot taka tesno integrirana s preostalimi rešitvami eZdravja. Omogoča različne entitete ter tipe entitet z ustrezno nastavljenimi elementi:

- uporabnik (delavci v zdravstvu, državljani, sistemski uporabniki, itd.)
- organizacija (izvajalec zdravstvene dejavnosti, ZZZS, itd.)
- aplikacija (aplikacija eZdravja)
- pravica oz. vloga

V sklopu Varnostne sheme se izvaja avtentikacija ter avtorizacija uporabnikov za rešitve eZdravja.

Spletna aplikacija za upravljanje s pravicami podpira naslednje funkcionalnosti:

- omogočeno je več nivojsko dodeljevanje pravic uporabnikom z možnostjo delegiranja administratorskih pravic za posamezno skupino uporabnikov,
- za vsako skupino kvalificiranih uporabnikov se določi nadzornika, ki ga določi in potrdi glavni nadzornik,
- nadzornik za posamezno skupino uporabnikov ima pravico urejati uporabnike, ki se uvrstijo v to skupino uporabnikov,
- uporabnik na najvišjem nivoju lahko preko aplikacije neposredno dodaja, odvzema, popravlja pravice uporabnikom tako na drugem kot na tretjem nivoju,
- uporabniki so o izvršitvi njihove zahteve za dodelitev pravic oziroma o odvzemu pravic obveščeni preko elektronskega naslova, ki ga vnese uporabnik ob posredovanju zahteve (vnese ga lahko tudi administrator). Na ta elektronski naslov uporabnika se pošiljajo vsa sporočila, povezana s pravicami.
- uporabnik za pravice zaprosi s svojim digitalnim potrdilom in z vnosom dodatnih informacij (podatkov),
- poleg identifikacije s kvalificiranim digitalnim potrdilom si uporabniki določijo še dodatno geslo, ki je potrebno za vstop v sistem,
- dostopi v sistem s kvalificiranim digitalnim potrdilom ter aktivnosti uporabnikov v postopku se beležijo in hranijo,
- omogočen je vpogled v čas in lokacijo zadnje uspešne in neuspešne uporabnikove prijave.

V okviru delovanja VS se izvajajo redne obdelave in sinhronizacije. Sinhronizacije se izvajajo na različne načine (XML tabele, spletni servisi, ipd.) iz naslednjih virov:

- Register izvajalcev zdravstvene dejavnosti in delavcev v zdravstvu (RIZDDZ) za potrebe uporabnikov in izvajalcev v zdravstvu, ter njihovih pooblastil
- RPPE



- ZZZS – za potrebe pooblastil delavcev v zdravstvu
- prevajalne tabele MJU za potrebe registracije certifikatov uporabnikov

Za potrebe integracije drugih rešitev z Varnostno shemo, le-ta omogoča naslednje vmesnike:

- sistem omogoča enotno avtentikacijo v okviru izvedbe postopka oz. seje (Single Sign-On), če so vključene različne aplikacije oz. moduli.
- sistem vključuje vmesnik, ki omogoča administracijo uporabnikov ter uporabo varnostne sheme tudi z uporabo spletnih storitev (WS). Preko vmesnika se z VS povezuje tudi delilnik bremen pri preverjanju pravice dostopa do zNET omrežja.
- na strani Varnostne sheme je za potrebe integracije aplikacij v Varnostno shemo implementirana spletna storitev za pridobivanje podatkov o uporabnikih in njihovih pravicah (SAML).

Druge funkcionalnosti, ki jih Varnostna shema omogoča so:

- OAUTH2 strežnik za podporo izvajanja SSO za REST spletne vmesnike in mobilne rešitve, ki je povezan na skupno bazo pravic
- XACML modul, ki omogoča upravljanje pravil tudi preko spletnega vmesnika

Okolje Varnostne sheme s pripadajočimi moduli in vmesniki, se izvaja v virtualnem okolju naročnika. Aplikacija se izvaja na dveh aplikacijskih strežnikih, ki delujeta v aplikacijski gruči v načinu Active/Active. Okolje izvajanja programske opreme je naslednje:

- Aplikacija teče na aplikacijskem strežniku JBoss 7.1.1 in je bila razvita v ogrodju Spring Framework
- Spletni vmesnik je razvit v tehnologiji .NET v programskem jeziku C#
- zbirka podatkov je Oracle 11 g
- OAUTH2 strežnik je na voljo kot odprtokodno programje

3. OBSEG JAVNEGA NAROČILA

V okviru javnega naročila se naroča:

- **A: Osnovno vzdrževanje** ohranja optimalno delujoče stanje informacijske rešitve Varnostna shema.

Osnovno vzdrževanje predvidoma zajema:

- zagotavljanje razpoložljivosti in zahtevane odzivnosti ter kakovosti izvajanja storitev vzdrževanja aplikativne programske opreme,
- zagotavljanje pravilnega delovanja aplikativne programske opreme,
- redno izvajanje in spremljanje postopkov in procedur za polnjenje uporabnikov v VS iz zunanjih virov,
- vzdrževanje vseh programskih in drugih komponent sistema, ki so potrebni za delovanje VS,
- izvajanje postopkov posodobitve vse programske opreme in komponent sistema, ki so potrebni za pravilno in varno delovanje VS (vključno z OAUTH2 strežnikom in XACML modulom),
- postopki izdelave in zagotavljanje varnostne kopije podatkov ter vzpostavitev ponovnega stanja delovanja pred vzrok za vrnitev v ponovno stanje delovanja



- (vzrok za uporabo varnostne kopije podatkov). Velja za celotno podatkovno zbirko kot tudi na nivoju posameznih entitet ali nastavitev posameznih modulov in komponent.
- vzdrževanje nastavljenih elementov rešitev, kot so šifranti, registri, enolični krajevnik virov (URL-ji), ...
 - analiza možnih izboljšav ali optimizacij rešitev ter izdelava predlogov za optimizacijo za naročnika,
 - reševanje napak pri delovanju v okviru predvidenega odzivnega časa,
 - sodelovanje z zunanjimi izvajalci pri iskanju možnih vzrokov za težave pri delovanju,
 - sodelovanje z zunanjimi izvajalci pri nadgradnji obstoječih rešitev,
 - sodelovanje z zunanjimi izvajalci pri vključevanju novih rešitev,
 - sodelovanje in usklajevanje z naročnikom,
 - vodenje evidence obsega del iz naslova sodelovanja z zunanjimi izvajalci zaradi vključevanja novih rešitev ali nadgradenj obstoječih rešitev,
 - priprava ponudb za dopolnilno vzdrževanje,
 - pomoč uporabnikom (drugi in tretji nivo podpore),
 - odkrivanje in odpravljanje skritih napak, varnostnih lukenj in pomanjkljivosti v kodi aplikativne programske opreme,
 - spremljanje tehnoloških novosti, povezanih z vzdrževano programsko opremo ter priprava predlogov in ukrepov za nemoteno delovanje oz. izboljšanje njenega delovanja,
 - objava novih verzij in novonastale dokumentacije, ki so posledica odprave napak in pomanjkljivosti, v repozitoriju naročnika in distribucija programerskim hišam,
 - reševanje problemov ter predlaganje ukrepov za nemoteno delovanje aplikativne programske opreme in optimizacijo delovanja,
 - preverjanje delovanja aplikacije na različnih okoljih,
 - ažurno vzdrževanje dokumentacije sistema,
 - redno preverjanje pravilnosti in optimalnosti delovanja sistema,
 - napredna administracija VS (urejanje aplikacij, ipd....) intervencije v primeru anomalij, ki jih zazna sam ali jih sporoči naročnik oz. uporabniki,
 - nudenje svetovanja in inštrukcij naročniku
 - učinkovito pomoč in svetovanje ključnim uporabnikom na strani naročnika,
 - migracija na drugo okolje
 - o ponudnik bo vsebinsko in tehnično svetoval ter nudil podporo pri prehodu na novo informacijsko rešitev
 - o ponudnik bo nudil podporo pri migraciji podatkov in nastavitev (npr. uporabniki v VS, poverilnice za izmenjavo podatkov, ipd.)
 - redno spremljanje delovanja rešitev in poročanje naročniku,
 - izdelava rednih in izrednih poročil o delovanju rešitve,
 - obveščanje naročnika ob zaznanih težavah,
 - nadzor sistema:
 - spremljanje in zbiranje dogodkov iz sistema;
 - periodično pregledovanje delovanja podatkovne zbirke;
 - stalno spremljanje delovanja podatkovnih virov integriranih na VS in ukrepanje v primeru morebitnih motenj;
 - tehnično usklajevanje s posameznimi podatkovnimi viri za zagotovitev operativnega delovanja;
 - predlogi ukrepov za preventivno reševanje;
 - upravljanje razpoložljivosti, zmogljivosti in kapacitete sistema:
 - spremljanje stanja in trendov sistema;
 - identificiranje kazalnikov oz. pokazateljev, preko katerih spremljamo, da obratovanje ni ogroženo;



- priprava predlogov in izvajanje ukrepov za zagotovitev zahtevane razpoložljivosti, zmogljivosti (optimizacija) in kapacitete;
 - koordinacija izvedbe ukrepov (obveščanje pristojnih oseb), posredovanje dogodka v izvajanje ustreznim izvajalcem;
- **B: Dopolnilno vzdrževanje** oziroma nadgradnja informacijske rešitve v dogovoru z naročnikom v primeru:
 - naknadno definiranih dopolnitev glede na spremembe v uporabniških zahtevah,
 - povezave oz. morebitne integracije z različnimi informacijskimi sistemi,
 - dodatnih potreb naročnika, ki bi se pokazale med uporabo rešitve,

Dopolnilno vzdrževanje predvidoma zajema:

- sodelovanje pri analizi in pripravi specifikacij uporabniških zahtev za dodajanje novih in izboljšanje obstoječih funkcionalnosti programske opreme,
- dopolnitve komponent rešitev zaradi nadgradnje obstoječih ali vključevanja novih rešitev,
- dopolnitve komponent rešitev zaradi optimizacije delovanja,
- dopolnitev dokumentacije rešitev po izvedenih dopolnitvah,
- izboljšanje obstoječih funkcionalnosti programske opreme, izboljševanje lastnosti delovanja, uporabnosti in dograjevanje novih funkcionalnosti ter modulov na podlagi predlogov naročnika, uporabnika ali izvajalca in s strani naročnika potrjenih specifikacij,
- prilagajanje programske opreme glede na spremembe systemskega okolja in operacijskega sistema v okviru možnosti in zagotovil proizvajalcev oziroma principalov ter glede na potrebe ostalih povezanih informacijskih sistemov,
- prilagajanje in dograjevanje programske opreme glede na vsebinske spremembe,
- priprava analitičnih izdelkov (poročila, statistike),
- odlaganje novih verzij, ki so posledica dopolnilnega vzdrževanja, v repozitorij naročnika in distribucija programerskim hišam,
- dokumentiranje novih verzij in funkcionalnosti, ki so rezultat dopolnilnega vzdrževanja,
- ostale aktivnosti po naročilu naročnika.

Izdelki, ki bodo realizirani z javnim naročilom in so odgovornost ponudnika rešitve:

- **Izdelki vodenja in kakovosti**
 - redna poročila o aktivnostih osnovnega in dopolnilnega vzdrževanja,
 - zapisi sestankov,
 - redna poročila o zmogljivosti, zanesljivosti ter varnosti sistema in uporabljene tehnologije,
- **Vsebinski in tehnični izdelki**
 - implementacija nadgradenj v okviru osnovnega in dopolnilnega vzdrževanja. Vse komponente programske opreme morajo vsebovati izvorno in izvršno kodo vseh modulov, obdelav in storitev.

4. TEHNOLOŠKE ZAHTEVE

- **Zahteve glede razpoložljivosti VS;**



- Rešitev mora delovati v režimu 24/7 in biti uporabnikom razpoložljiva vsaj 99,8% časa (kar predstavlja 17,52 ur nenapovedanega izpada v tem na letni ravni). Izpad v obdobju enega meseca ne sme presežati 2 ur. Izpad v obdobju enega tedna ne sme presežati 30 minut.
- **Zahteve glede zmogljivosti (odzivnosti);**
 - Razpoložljivost rešitve vpliva na proces zdravljenja pacientov in delo izvajalcev zdravstvenih storitev, zato mora rešitev ob normalnem delovanju omrežnih in sistemskih storitev delovati v realnem času in zagotavljati, da je ob normalnem delovanju omrežnih in sistemskih storitev odzivni čas pod 1 sekundo.
 - VS mora biti sposobna sprejeti do 5000 transakcij na uro brez bistveno zmanjšane odzivnosti ali bistvenega padca performanc.
 - Odzivni čas spletne rešitve ne sme ob normalnem delovanju omrežnih in sistemskih storitev presežati 2 sekundi.

5. ZAHTEVE GLEDE ODZIVNEGA ČASA

- **Zahteve glede odzivnega časa pri reševanju zahtevkov**

Ponudnik bo pri opravljanju storitev osnovnega vzdrževanja zagotovil reševanje zahtevkov v primeru napak oz. motenj pri delovanju glede na njihovo prioriteto v skladu z odzivnimi časi v spodnji tabeli.

Prioriteta zahtevka	Odzivni čas	Čas, v katerem mora izvajalec odpraviti vzroke za napako oz. motnjo
kritična	1 ura	2 uri
visoka	2 uri	4 ure
pomembna	4 ure	8 ur
nizka	1 delovni dan	2 delovna dneva

Tabela 1: Odzivni časi v primeru zahtevkov zaradi napak oz. motenj

Napaka	Vpliv	Opis
kritična	zelo visok vpliv	Popolna odpoved delovanja storitev ali poglobitnega dela storitev, ki preprečuje uporabo ključnih delov informacijske rešitve vsem uporabnikom.
visoka	visok vpliv	Delna odpoved delovanja storitev ali poglobitnega dela storitev, ki resno vpliva na uporabo ključnih delov informacijske rešitve skupini uporabnikov.
pomembna	srednji vpliv	Oteženo delovanje storitev, ki ne



		vpliva kritično na uporabo ključnih delov informacijske rešitve pri skupini ali posameznem uporabniku.
nizka	nizek vpliv	Katerikoli incident, ki ne vpliva na uporabo ključnih delov informacijske rešitve.

Tabela 2: Določitev stopnje napake

- **Odzivni čas za dopolnilno vzdrževanje:**

V primeru povpraševanj naročnika za dopolnilno vzdrževanje je ponudnik dolžan pripraviti ponudbo najkasneje v treh delovnih dneh, v kolikor ni pisno dogovorjeno drugače. Ponudba vsebuje predlog izvedbe s podrobnim načrtom potrebnih aktivnosti in z oceno obsega del.

- **Drugo:**

Ponudnik je dolžan na vprašanja ponudnikov pri integraciji novih rešitev ali nadgradnji obstoječih podati odgovor na vprašanje najkasneje v enem delovnem dnevu.

6. NEFUNKCIONALNE ZAHTEVE

Za dobro komunikacijo in kvalitetno izvajanje nalog je potrebno upoštevati naslednja pravila.

1. Vodenje pogodbenega odnosa za izvajanje nalog se uporablja aplikacija Redmine (<https://redmine.ezdrav.si>). V Redmine se vodijo:

- nove funkcionalnosti,
- napake,
- podpora,
- testiranje,
- ostale naloge,
- zapisniki sestankov,
- mesečna in ostala poročila (o testiranju, o incidentih, o opravljenih delih...) - vsaj povezave do fizičnih oblik poročil.

2. Vodijo se verzije rešitev v skladu z določili Semantic Versioning 2.0.0 (<http://semver.org/>). Pri vodenju različic velja:

- številke različice se vodi MAJOR.MINOR.PATCH, prirastek:
- MAJOR/GLAVNA različica ko bo nezdružljive spremembe API,
- MINOR/MANJŠA različica ko dodate funkcionalnost v nazaj združljiv način, in



- PATCH /POPRAVEK različica ko bo nazaj združljive popravke.
 - Dodatne oznake za predhodno izpustitev in gradijo metapodatki so na voljo kot razširitve formata MAJOR.MINOR.PATCH.
 - Glavno različico se vpeljuje dvakrat (2.) (potencialno lahko porušimo delovanje za nazaj). Izjeme tega pravila se sproti uskladi z vsemi vpletenimi.
 - Manjšo različico se lahko vpeljuje pogosteje (ne rušijo funkcionalnosti za nazaj).
 - Popravke se vpeljuje po potrebi.
3. Predvideva se delovanje vsaj treh okolij
- Razvojno okolje je lahko pri pogodbenem izvajalcu, ki zagotovi dostop naročniku,
 - Testno okolje mora biti nameščeno na naročnikovi infrastrukturi,
 - Produktijsko okolje je nameščeno na naročnikovi infrastrukturi,
 - Testno okolje mora vsebovati enake gradnike kot okolje redne uporabe (produkcija).
4. Odložišče programske kode je Apache Subversion v eZdravje okolju (<https://koda.ezdrav.si>), ki zahteva potrjevanje sprememb in vodenje različic s strani izvajalca pogodbenega odnosa.
- Operacija commit mora vsebovati enolični identifikator naloge v sistemu Redmine
 - Operacija commit naj se izvaja sproti in redno
 - Za potrebe verziniranja je potrebno ob vsakem zaključku razvoja za katerkoli od oznak MAJOR, MINOR ali PATCH, ustvariti nov TAG v imeniku tags v SVN. Na ta način je vedno mogoč prehod na predhodno različico ali katerokoli drugi različico kode.
 - Razvoj poteka vedno v imeniku trunk znotraj SVN.
 - Za potrebe razvoja funkcionalnosti se po potrebi ustvarja ločene veje oz. branch-e, ki se jih kasneje merge-a oz. združi s trunk verzijo.
 - Plačilo računov je vezano na naloge v Redmine, ki morajo biti potrjeno zaključene. To pa pomeni tudi, da morajo biti na naloge povezane tudi spremembe v programski kodi.
5. Izvajalec se mora pri razvoju rešitev držati pravil lepega programiranja in obvezno v izvorni kodi opisati metode, funkcije, objekte in spremenljivke z nazornim opisom.
- Naročnik bo naključno preverjal upoštevanje pravil.
6. Izvajalec mora pred uvedbo nove različice rešitve narediti in prikazati test nove različice rešitve, ki je tehnično dokumentiran.
- Delovanje mora prikazati vsaj na testnem okolju pri naročniku



7. Razpoložljivost, stabilnost, skalabilnost in odzivni časi rešitev so določene v tehničnih specifikacijah pogodbenega odnosa.
8. Izvajalci so dolžni obveščati o koristnih in nujnih nadgradnjah, da se izognemo zastaranju in da zagotavljamo varno in vzdržno delovanje rešitev.
9. Izvajalci so dolžni obveščati o vseh predvidenih in nastalih težavah pri uporabi in izvajanju pogodbenega odnosa.
10. Tehnična dokumentacija mora vsebovati grafične predstavitve, kjer je to smiselno (UML, BPMN2, sheme, ...).
11. Pri nadgradnjah mora izvajalec dopolnjevati končne različice dokumentacije (ne samo spremembe). To velja tako za uporabniško kot tudi za tehnično dokumentacijo ter grafične predstavitve.
12. Izvajalec je dolžan sporočiti informacije, spremembe in odgovore na vprašanja o rešitvah ter sporočiti posege, ki vplivajo na izpad delovanja na prvi nivo podpore.
13. Podpisovanje dokumentov mora biti elektronsko.
14. Vsak izvajalec 2. Nivoja podpore je dolžan sodelovati s 1. nivojem podpore.
15. Vsebinske definicije je potrebno črpati iz Terminološkega slovarja NIJZ.

7. DRUGE ZAHTEVE

Ponudnik mora poskrbeti, da bo z dnem začetka pogodbe, začel operativno izvajati storitve vzdrževanja, ter da bo posedoval ustrezna znanja za izvajanje pogodbe, s čimer bo zagotovil čim bolj kvalitetno izvajanje vzdrževalnih storitev, s tem pa tudi kvaliteto izvajanja predmetne storitve.

- **Baza znanja**

Ponudnik mora vzdrževati t.i. bazo znanja, v kateri bo hranil podatke pomembne za vzdrževanje oz. izvajanje rešitve, ki v preostali dokumentaciji niso zajeti. Bazo znanja ob izteku pogodbe preda naročniku ter novemu izvajalcu po potrditvi naročnika.

Spodaj podpisani pooblaščen predstavnik ponudnika izjavljam, da vse ponujene storitve v celoti ustrezajo zgoraj navedenim opisom.

V/na _____, dne _____

Ime in priimek:

Žig in podpis: