TEHNIČNE SPECIFIKACIJE ZA JAVNO NAROČILO

NMV5704/2014

Storitve vzdrževanja, dopolnilnega vzdrževanja ter nadgradenj Portala in Varnostne sheme MDDSZ

KAZALO

1. UPORABNOST IN NAMEN PORTALA TER VARNOSTNE SHEME MDDSZ

Portal MDDSZ in Varnostna shema omogočata vzpostavitev enotne vstopne točke za zbir aplikacij ter elektronskih vlog, z možnostjo upravljanja uporabnikov in njihovih dostopov ter ustreznimi podpornimi vsebinami:

- dostop do aplikacij v informacijskem sistemu centrov za socialno delo (IS CSD),
- sistem nadzora delovanja informacijskih sistemov MDDSZ z možnostjo nastavitev različnih statusov (semafor),
- vzpostavitev javnega in zaprtega dela Portala s funkcionalnostmi spletne strani pomoči, novic, opisov aplikacij, statistik in aktualnih zbirov.

Uvedba Portala MDDSZ izboljšuje varnost podatkov v informacijskih sistemih MDDSZ (tistih, ki so vključeni v Varnostno shemo), saj je dostop možen le s pomočjo digitalnega potrdila in gesla. Različne funkcionalnosti Portala MDDSZ omogočajo boljši in transparentnejši pretok informacij ter boljšo participacijo uporabnikov.

Izvajanje nadzora nad uporabniki IS CSD ter avtorizacija pravic za dostop do aplikacij se izvaja z uporabo Varnostne sheme.

2. OPIS FUNKCIONALNOSTI IN VSEBIN PORTALA TER VARNOSTNE SHEME MDDSZ

2.1 Vzpostavitev javnega in zaprtega dela Portala z dostopom do aplikacij informacijskega sistema centrov za socialno delo (IS CSD)

Dostop do aplikacij IS CSD v zaprtem omrežju javne uprave (HKOM) je mogoč z digitalnimi spletnimi potrdili, dostop do določenih podatkov na zunanjem Portalu pa z registriranim dostopom s pomočjo uporabniškega imena in gesla.

2.2 Sistem nadzora delovanja informacijskih sistemov MDDSZ z možnostjo nastavitev različnih statusov (semafor)

Informiranje uporabnikov o delovanju posameznega informacijskega sistema MDDSZ je realizirano z izrisom Semaforja, ki se izrisuje vsakemu uporabniku posebej za posamezne informacijske sisteme MDDSZ, ki jih trenutno lahko uporablja. Prikazano je ime informacijskega sistema, status (deluje, ne deluje, zaprto za vnos, ali drugi statusi, ki jih želimo prikazati) in drugi poljubni podatki.

V sklopu semaforja so prikazani tudi vsebinski in tehnični skrbniki posamezne aplikacije informacijskih sistemov MDDSZ. Semafor prikazuje status delovanja informacijskega sistema MDDSZ po vnaprej določenem časovnem intervalu.

2.3 Vzpostavitev Portala s funkcionalnostmi spletne strani

Portal MDDSZ omogoča objavo in prikaz naslednjih vsebin:

- tehnična navodila,
- vsebinska navodila,
- obvestila za uporabnike Portala,
- povezave na vsebino in papirne vloge,
- informativni izračuni,
- prikaz web statistik

in podpira tudi druge funkcionalnosti:

- omogočeno je hkratno obveščanje vseh uporabnikov,
- MDDSZ administratorji imajo vpogled v težave in odgovore,
- izvaja se e-mali management,
- omogočeni so prednastavljeni odgovori na vprašanja,
- spremlja se obisk Portala in izvajajo se statistike,
- podprta je zbirka znanja,
- podprto je objavljanje novic.

Tehnična navodila
Objavljati je mogoče tehnična navodila uporabnikom aplikacij za posamezno ali za več aplikacij hkrati. Navodila lahko objavljajo uporabniki na strani pogodbeno vezanih zunanjih izvajalcev in po potrebi tudi administratorji MDDSZ.
Omogočeno je prikazovanje zgodovine obvestil.
Namen je omogočiti transparenten in ažuren prikaz navodil na enem mestu.

Vsebinska navodila
Objavljati je mogoče vsebinska navodila uporabnikom aplikacij za posamezno ali za več aplikacij hkrati. Navodila lahko objavljajo uporabniki MDDSZ in po potrebi tudi administratorji MDDSZ.
Omogočeno je prikazovanje zgodovine obvestil.
Namen je omogočiti transparenten in ažuren prikaz navodil na enem mestu.

Obvestila za uporabnike Portala
Objavljati je mogoče vsebinska in tehnična obvestila o delovanju posameznih aplikacij in tudi vsebinskih posebnosti v določenem časovnem obdobju kot tudi sezname in gradiva glede na aktualne napotke in dogodke.
Obvestila se lahko objavljajo ločeno za vsako aplikacijo IS CSD posebej ali pa skupno za vse uporabnike. Obvestila praviloma objavljajo administratorji MDDSZ.

Povezave na vsebino in papirne vloge
Navedene so povezave, ki po vsebini spadajo v delovno področje, ki ga pokrivajo aplikacije IS CSD. Glede na potrebe uporabnikov, se lahko dodajale nove.

Informativni izračuni
Prikazovati je mogoče podatkovne izračune, ki so pripravljene na podlagi obdelav podatkov iz aplikacij IS CSD. Predvideni so tudi izvozi podatkov v različnih oblikah.

Prikaz web statistik
Prikazovati je mogoče grafične in podatkovne statistike, ki so pripravljene na podlagi podatkov iz aplikacije IS CSD.

2.4 Varnostna shema in sistem upravljanja uporabnikov

Varnostna shema je zasnovana kot centralna varnostna shema uporabnikov v postopku.

Poleg avtentikacije uporabnikov se v sklopu Varnostne sheme upravljajo tudi vse avtorizacije uporabnikov. Rešitev je primerna tudi za uporabo v drugih aplikacijah (modularna rešitev).

Spletna aplikacija za upravljanje s pravicami podpira naslednje funkcionalnosti:

- omogočeno je večnivojsko dodeljevanje pravic uporabnikom z možnostjo delegiranja administratorskih pravic za posamezno skupino uporabnikov,
- za vsako skupino kvalificiranih uporabnikov se določi administratorja, ki ga določi in potrdi glavni administrator,
- administrator za posamezno skupino uporabnikov ima pravico dodajati in brisati 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 postopki.
- 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,
- podprt je postopek samodejnega dodeljevanja novega gesla uporabniku, ki je pozabil prejšnje geslo,
- omogočen je vpogled v čas in lokacijo zadnje uspešne in neuspešne uporabnikove prijave,
- omogočeno je avtomatsko zaklepanje uporabniku v primeru prevelikega številka neuspešnih poskusov prijav ter možnost odklepanje uporabnika administratorju.

Sistem omogoča enotno avtentikacijo v okviru izvedbe postopka oz. seje (SSO), če so vključene različne aplikacije oz. moduli.

Sistem vključuje vmesnik, ki omogoča administracijo uporabnikov ter uporabo varnostne sheme tudi z uporabo spletnih storitev (WS).

Izvajajo se redne sinhronizacije uporabnikov Varnostne sheme ter uporabnikov aplikacij ISCSD in ISCSD2 (IS CSD).

Baza Varnostne sheme je povezana z MJU prevajalnimi tabelami za potrebe registracije certifikatov uporabnikov.

3. UPORABNIKI, KI UPORABLJAJO PORTAL IN VARNOSTNO SHEMO MDDSZ TER DOSTOPNE VSEBINE

3.1 Uporabniki Portala MDDSZ

Skupine (evidentiranih) uporabnikov, ki uporabljajo notranji del Portala in Varnostno shemo MDDSZ (HKOM) so:

- uporabniki MDDSZ,
- uporabniki na strani pogodbeno vezanih zunanjih izvajalcev,
- uporabniki na strani vzdrževalca Portala MDDSZ,
- notranji uporabniki aplikacij IS CSD (CSD, Javni sklad RS za razvoj kadrov in štipendije (v nadaljevanju sklad),..),
- zunanji uporabniki aplikacij IS CSD (izplačevalci, kot so občine, MIZŠ, upravne enote),

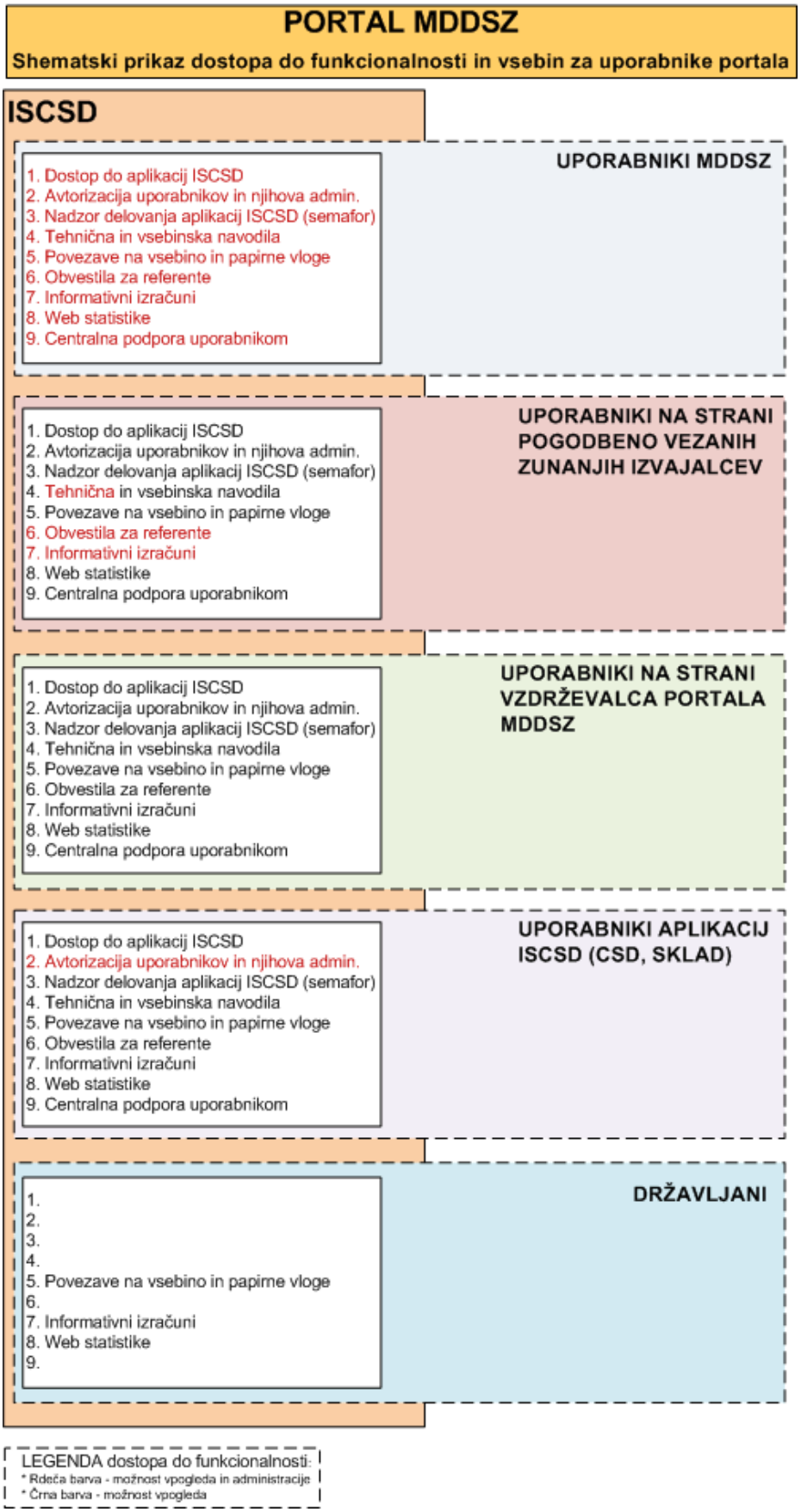
nato pa so še uporabniki zunanjega dela Portala:

- državljani (iskanje informacij, uveljavljanje pravic).

Uporabniki notranjega dela Portala in njihove pravice so definirane v Varnostni shemi.

Prikaz vsebin na Portalu MDDSZ je definiran glede na razvrstitev uporabnika, ki vstopa na Portal MDDSZ. Trenutno je definiranih pet skupin uporabnikov.

SLIKA: Shematski prikaz dostopa do funkcionalnosti in vsebin za uporabnike Portala:



3.2 Dostopne vsebine na Portalu MDDSZ

Nekatere vsebine so javno dostopne, druge pa le določenim pooblaščenim uporabnikom.

Vsebine, ki so namenjene evidentiranim (prijavljenim) uporabnikom v Varnostni shemi, so vsebinsko ustrezno prilagojene posameznemu uporabniku. Uporabnik ima na voljo le informacije, ki jih potrebuje. Ob prijavi ima omogočen dostop do spletne programske opreme po principu enkratne prijave.

Vstop na strani namenjene evidentiranim uporabnikom je izveden z uporabo certifikata SIGOV-CA ter SIGEN-CA in je namenjenemu uporabi v javni upravi.

Vsebine, ki so namenjene javnosti (državljani), so javno dostopne in jih lahko pregleduje vsak registrirani uporabnik. Dodajajo in urejajo se glede na potrebe posamezne skupine uporabnikov. Dostopne

3.3 Uporabniki aplikacijskega modula Varnostne sheme (VS)

Uporabniki in njihove pravice so definirane v Varnostni shemi in so tudi uporabniki aplikacij IS CSD in so sledeči:

- Direktorji CSD-jev
- Uporabniki MDDSZ s skrbniškimi pravicami
- uporabniki na strani vzdrževalca VS in Portala MDDSZ
- izplačevalci in uporabniki Distribucijskega modula (DM), kot so občine, MIZŠ, upravne enote

3.4 Tehnična pomoč

Na vstopni strani Portala so vsem uporabnikom Portala na voljo uporabniška navodila, ki uporabniku opišejo vse funkcionalnosti sistema in so prilagojena vsem vrstam uporabnikov.

4. ARHITEKTURA SISTEMA IN TEHNOLOŠKO OKOLJE PORTALA TER VARNOSTNE SHEME MDDSZ

4.1 Splošne arhitekturne in tehnološke smernice

Portal MDDSZ, Varnostna shema in vsi aplikativni moduli v okviru Portala MDDSZ so nameščeni na infrastrukturo, ki se nahaja na Ministrstvu za javno upravo (MJU) Tržaška cesta 21, 1000 Ljubljana in je v uporabi MDDSZ. Tehnologije in programske opreme za razvoj aplikativnih modulov Portala MDDSZ in Varnostne sheme morajo biti skladne s tehnologijami (operacijski sistem, razvojna programska oprema, podatkovna baza), ki delujejo na MJU.

Izvajalec mora upoštevati splošne usmeritve in podrobnosti, ki se nahajajo v dokumentu Generične_Tehnološke_Zahteve_–_GTZ_v1.11.2.doc s posebnim poudarkom na naslednjih poglavjih:

- Tehnološko okolje;
- Tehnološki standardi in specifikacije;
- Tehnološka neodvisnost na strani odjemalcev;
- Splošne arhitekturne smernice;
- Splošna postavitvena pravila;
- Način dostopa do podatkovne zbirke;
- Metodologija razvoja ter upravljanje s spremembami programske opreme;
- Vsebina dokumentacije in napotki za izdelavo;
- Optimalnost aplikacije in baznih objektov:
- Namestitvena pravila;
- Nadzorni podatki: sistemsko / aplikacijski nivo;
- Revizijske sledi;
- Informacijska varnost in skladnost z zakonodajo.

4.2 Implementirane tehnološke rešitve Portala in Varnostne sheme MDDSZ

Portal MDDSZ in Varnostna shema sta postavljena v testnem in produkcijskem okolju na MJU v povezavi z obstoječimi FORMS aplikacijami sistema IS CSD v okolju:

- Web strežnik: prilagojena verzija LiffeRay portala 5.2.3,
- aplikacijski strežnik: Oracle WebLogic 11gR1 10.3.4,
- podatkovni strežnik: Oracle DB 11g R2 11.2.0.2.

Za aplikacijski nivo sistema je vzpostavljeno javansko strežniško izvajalno J2EE okolje.

Pri razvoju Portala MDDSZ in Varnostne sheme so uporabljene naslednje rešitve:

- SSL (Secure Sockets Layer), splošno sprejet varnostni protokol,
- Enovito upravljanje in prijava uporabnikov (SingleSignOn - SSO),
- infrastruktura javnih ključev ali Public Key Infrastructure (PKI).

Skalabilnost in zanesljivost: sistem je zasnovan tako, da je mogoče z uporabo strojne opreme oz. konfiguracij strojne opreme povečati njegovo maksimalno obremenitev ter njegovo zanesljivost.

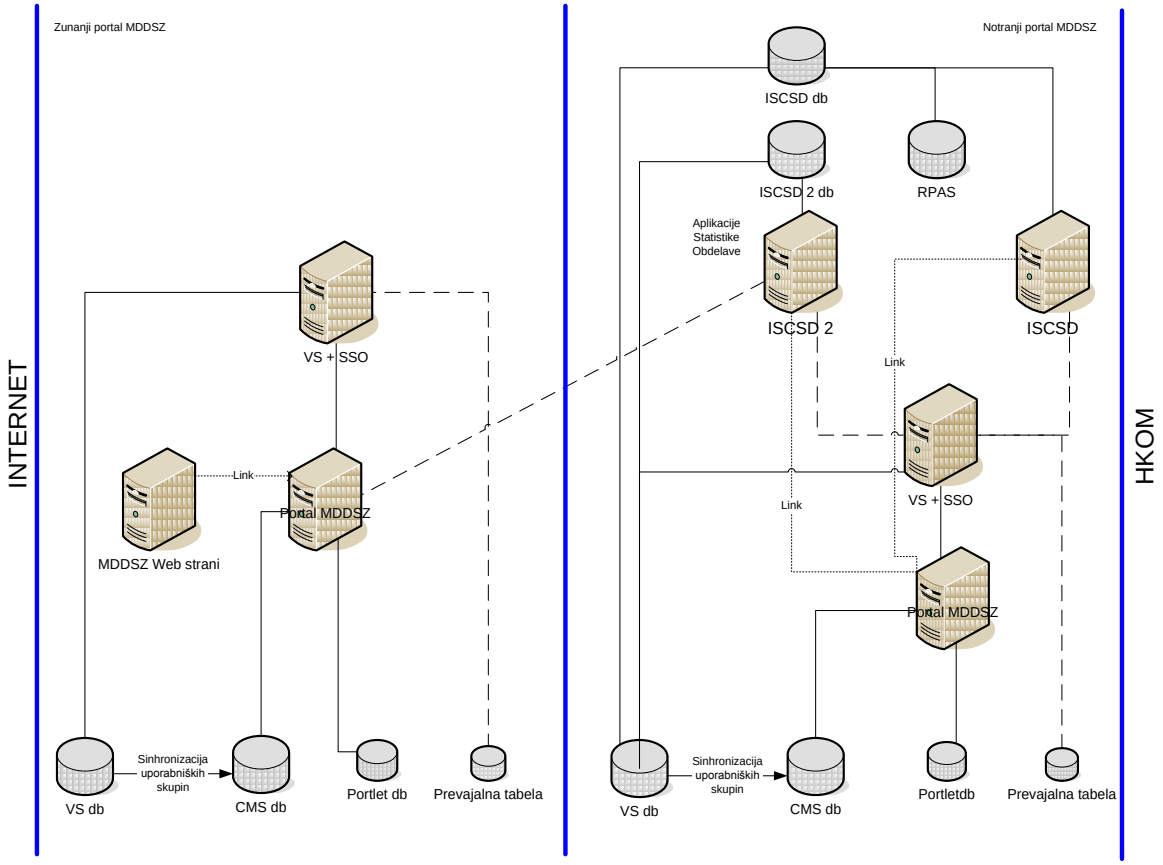
Izvedena je integracija uporabe certifikatov SIGOV-CA in SIGEN-CA v Varnostno shemo za uporabnike zaprtega dela Portala, dostop tudi z ostalimi veljavnimi certifikati (v Sloveniji priznana kvalificirana digitalna potrdila kot na primer: SIGOV-CA ali SIGEN-CA za fizične osebe ali za zaposlene pri pravnih osebah, POŠTA®CA, AC-NLB, HALCOM CA FO ali HALCOM CA PO) pa je možen za uporabnike odprtega dela Portala MDDSZ.

Pri izvajanju projekta mora izbrani izvajalec upoštevati postopke in dokumentacijo, ki je zahtevana v dokumentu Generične_Tehnološke_Zahteve_–_GTZ_v1.11.2.doc, torej dokument RTP_Politika v zvezi z namestitvami informacijskih sistemov na skupno strežniško infrastrukturo.doc in naslednje obrazce:

- PRILOGA_RTP_1_Profil aplikacije
- PRILOGA_RTP_3_Obrazec za vzpostavitev spletišča_aplikacije OVSA01
- PRILOGA_RTP_4_Naročilo za namestitev aplikacije_popravka OVSP

Varnostna shema komunicira s Portalom MDDSZ preko spletnih servisov in ima odprte poti do: Portala MDDSZ, vseh IS CSD aplikacij in podatkovnih baz, ki so na spodnji sliki.

SLIKA: Logična slika poteka sporočil med aplikacijami

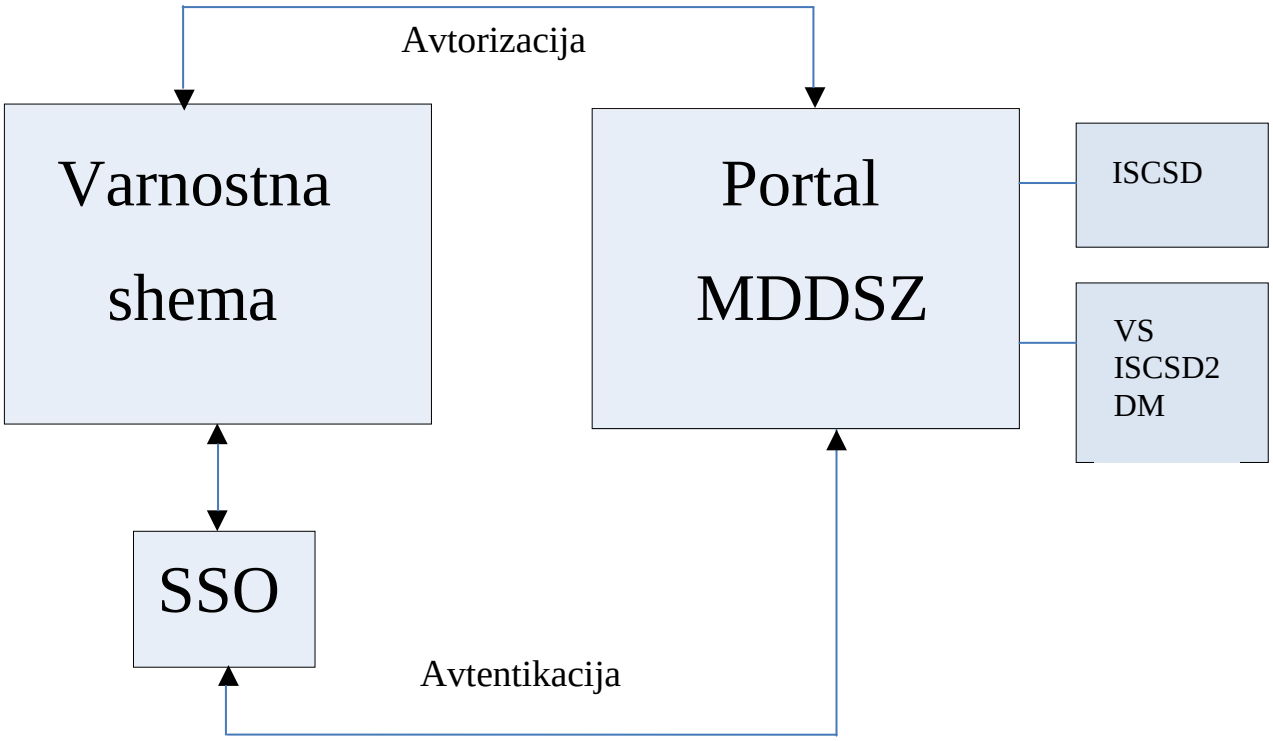


5. SPECIFIKACIJA VMESNIKA ZA INTEGRACIJO APLIKACIJ Z VARNOSTNO SHEMO

5.1 Integracija Portala in Varnostne sheme MDDSZ

Modul Varnostna shema (VS) se v sklopu Portala MDDSZ uporablja za administracijo uporabnikov različnih aplikacij.

SLIKA: Umestitev Varnostne sheme v kontekst Portala MDDSZ



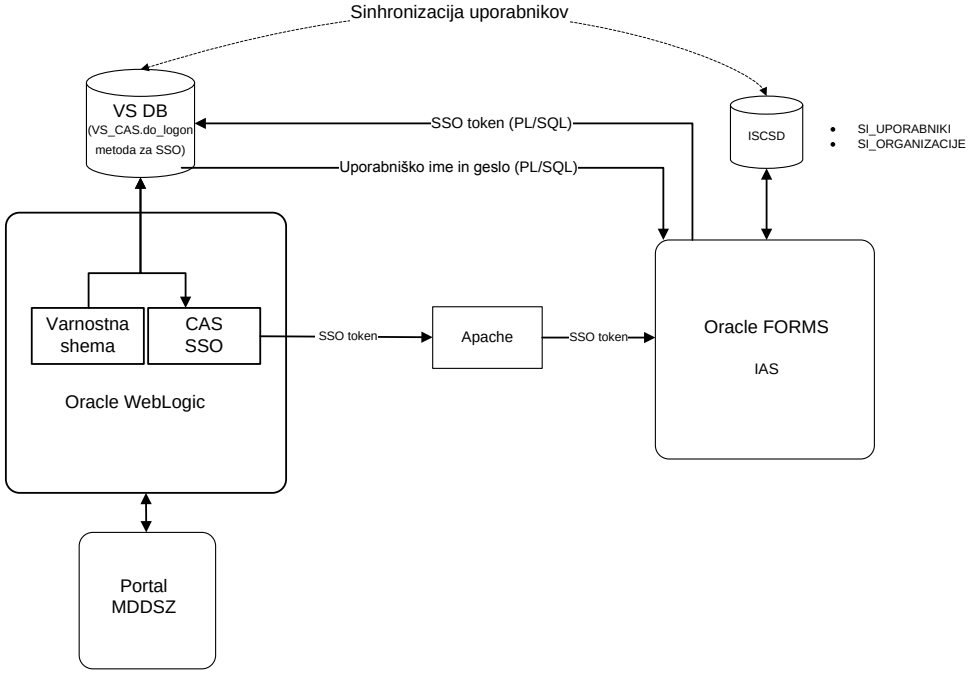
Varnostna shema zagotavlja administracijo uporabnikov in njihovih vlog na posameznih aplikacijah, do katerih se dostopa preko Portala MDDSZ.

SSO je mehanizem za enkratno prijavo uporabnika v vse aplikacije, do katerih ima nastavljene pravice, s čimer se izognemo prijavi v vsako aplikacijo posebej. Posamezne aplikacije imajo možnost nastavitve, da se eksplicitno od uporabnika zahteva ob prijavi tudi geslo. SSO izvede avtentikacijo uporabnikov.

5.2 Način integracije Oracle Forms aplikacij z Varnostno shemo

Integracija Oracle Forms aplikacij z Varnostno shemo je izvedena preko komponente Jasig CAS

SLIKA: integracija preko Jasig CAS poteka na sledeč način:



Način integracije Oracle Forms aplikacij s SSO preko Varnostne sheme:

1. Uporabnik preko Portala MDDSZ zahteva dostop do aplikacije.
2. Varnostna shema izvede avtentikacijo uporabnika na podlagi uporabnikovega certifikata, SSO komponenta pa Oracle Forms aplikaciji preko Apache http strežnika pošlje kriptiran SSO token (žeton).
3. Oracle Forms aplikacija kriptirani SSO token posreduje v Varnostno shemo, ki aplikaciji vrne uporabniško ime in geslo uporabnika. Gesla bodo v Varnostni shemi kriptirana z močno 3-DES enkripcijo.

Aplikacija, ki želi uporabljati SSO (Single sign on), svojo prijavno stran preusmeri na naslov https://vs.sigov.si/sso/login?service={returnURL}. Varnostna shema preveri ali je uporabniško digitalno potrdilo prijavljeno v Varnostno shemo. Nato vrne SSO žeton s katerim aplikacija pridobi podatke o uporabniku in njegove pravice na tej aplikaciji. Vrednost žetona se aplikaciji vrne preko redirecta na {returnURL}.

V primeru, ko certifikat še ni prijavljen v Varnostno shemo, se prikaže stran za prvo prijavo, kjer uporabnik lahko vnese svojo kandidaturo za uporabo aplikacij registriranih v Varnostno shemo. Po potrditvi kandidature s strani administratorja prijava poteka na zgoraj opisan način.

Glede na dogodke v Varnostni shemi, se periodično posodablja tabelo uporabnikov in organizacij v bazi Oracle Forms aplikacij. Posodabljanje poteka preko baznih procedur.
Varnostna shema deluje skladno z njenim modularnim in splošnim konceptom za vse aplikacije v javni upravi in praviloma ne potrebuje parcialnih rešitev za posamezne aplikacije.

5.3 Vmesnik spletne storitve na strani APLIKACIJ

Na strani Varnostne sheme je za potrebe integracije drugih aplikacij v Varnostno shemo implementiran spletni servis za pridobivanje podatkov o uporabnikih in njegovih pravicah.

5.4 Vmesnik spletne storitve za administracijo uporabnikov

Na strani Varnostne sheme je implementirana spletna storitev v skladu s predpisano shemo, ki jo morajo implementirati odjemalci (aplikacije) za klice te storitve.

5.5 Varnost med sodelujočimi informacijskimi sistemi

Vse strani vpletene v komunikacijo z aplikacijo Varnostna shema morajo podpirati protokol HTTPS za vzpostavitev varne povezave med sodelujočimi informacijskimi sistemi. Uporabnik spletnega servisa se mora identificirati z veljavnim digitalnim potrdilom (certifikatom), ki je registriran v sistemu Varnostni shemi kot sistemski uporabnik.

Pri vzpostavitvi integracije s posamezno aplikacijo je potrebno izmenjati informacije o javnih ključih digitalnih potrdil, ki bodo uporabljena tako za vzpostavitev varne SSL seje (strežniška digitalna potrdila) kot za avtentikacijo klicateljev (odjemalska digitalna potrdila).

5.6 Obravnavanje napak

Določene operacije, vrednosti vhodnih parametrov, poslovna pravila, itd. lahko povzročijo, da spletna storitev ne bi mogla izvesti želene operacije. Varnostna shema ob prejemu paketa preveri skladnost s predpisano shemo ter v primeru napake javila napako. Sistemske napake kot so npr. nezadostne pravice, nedostopnost podatkovne baze in podobno so klicatelju sporočene preko mehanizma soap fault. Vsaka napaka ima tudi opisni del z sporočilom napake.

6. VZDRŽEVANJE PORTALA IN VARNOSTNE SHEME MDDSZ

Vzdrževanje Portala MDDSZ in Varnostne sheme obsega naloge, ki se izvajajo v okviru osnovnega vzdrževanja za redno delovanja sistema in dopolnilnega vzdrževanja. Izvajalec mora zagotavljati:

- pravilno delovanje Portala in Varnostne sheme,
- preverjanje pravilnosti in optimalnosti delovanja sistema,
- intervencije v primeru anomalij, ki jih zazna sam ali jih sporoči naročnik oz. uporabniki,
- usklajevanje s sistemsko službo,
- učinkovito pomoč in svetovanje ključnim uporabnikom na strani naročnika,
- oblikovanje in podajanje predlogov za optimizacijo delovanja,
- prilagoditve in posege v skladu z naročili in potrebami naročnika.

6.1 Osnovno vzdrževanje za redno delovanja sistema

Osnovno vzdrževanje sistema se izvaja v okviru mesečnega pavšala, je vezano neposredno na aplikacijo oz. kodo in storitve se izvajajo v okviru obstoječih funkcionalnosti aplikacije.

Podrobnejši opis predvidenih storitev osnovnega vzdrževanja:

- zagotavljanje razpoložljivosti in zahtevane odzivnosti ter kakovosti izvajanja storitev vzdrževanja aplikativne programske opreme,
- pomoč uporabnikom - daljinska pomoč pri reševanju težav uporabnikov ter odgovarjanje na vprašanja glede uporabe vzdrževane programske opreme. O nastalih napakah in končni odpravi izvajalec obvešča naročnika in njegovo tehnično službo,
- svetovanje ključnim uporabnikom,
- odkrivanje in odpravljanje skritih napak in pomanjkljivosti v kodi aplikativne programske opreme po preteku testnega obdobja oziroma jamstva iz pogodbe o nakupu, prevzemu oziroma izdelavi aplikativne programske opreme, razen odpravljanja skritih napak in pomanjkljivosti v nadgradnjah aplikativne programske opreme, ki bodo morebiti izvedene v okviru tega naročila (pogodbe),
- 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 SVN repozitoriju naročnika,
- reševanje problemov ter predlaganje ukrepov za nemoteno delovanje aplikativne programske opreme,
- preverjanje delovanja aplikacije na različnih okoljih,
- ažurno vzdrževanje dokumentacije sistema.

Osnovno vzdrževanje poteka do izteka pogodbe.

Predvideni odzivni časi:

Prioriteta zahtevka	Odzivni čas*	Čas v katerem mora izvajalec odpraviti napako**	Primer
kritična	Takoj, ko je mogoče - začne reševati takoj	4 ure	Sistem ne deluje v celoti.
visoka	4 ure	8 ur	Sistem deluje deloma, ogrožene so nekatere pomembne funkcionalnosti
pomembna	8 ur	18 ur	Sistem deluje deloma, ogrožene so le nekatere manj bistvene funkcionalnosti
nizka	1 delovni dan	2 delovna dneva	Lepotne napake

*Odzivni čas - je maksimalni čas, ki preteče od trenutka, ko uporabnik izvajalcu pošlje zahtevek za odpravo napake do trenutka, ko izvajalec na zahtevek odgovori in prične z reševanjem napake.
**Čas, v katerem mora izvajalec odpraviti napako - je maksimalni čas od trenutka, ko uporabnik izvajalcu pošlje zahtevek za odpravo napake do trenutka, ko izvajalec odpravi napako.

Problem opredeljujemo kot težavo oziroma določeno nezaželeno stanje, ki ni skladno s pričakovanji in ga je potrebno odpraviti oziroma rešiti, na ta način, da se stanje normalizira.

Uporabniško vprašanje predstavlja problem, ki je logična celota, katerega se rešuje praviloma daljinsko (npr. telefonski klic, e-mail oziroma z namensko spletno aplikacijo za podporo uporabnikom) in se za njegovo rešitev porabi do 15 minut.

Motnja predstavlja problem, ki je logična celota, katerega se rešuje praviloma daljinsko (npr. telefonski klic, e-mail oziroma z namensko spletno aplikacijo za podporo uporabnikom) in se za njegovo rešitev porabi do 30 minut.

6.2 Dopolnilno vzdrževanje

Dopolnilno vzdrževanje aplikativne programske opreme je (podobno kot osnovno vzdrževanje) vezano neposredno na aplikacijo oz. kodo in zajema izgradnjo novih funkcionalnosti aplikacije ter dopolnjevanje obstoječih funkcionalnosti aplikacije.

Podrobnejši opis predvidenih storitev dopolnilnega vzdrževanja:

- sodelovanje pri analizi in pripravi specifikacij uporabniških zahtev za dodajanje novih in 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 sistemskega 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 oziroma sprememb in dograditev programske opreme v SVN repozitorij naročnika,
- dokumentiranje novih verzij in funkcionalnosti, ki so rezultat dopolnilnega vzdrževanja.

Dopolnilno vzdrževanje se izvede po predhodnem pisnem naročilu naročnika, ki je lahko tudi elektronska pošta. Če izvajalec izvede funkcionalnost brez naročila naročnika, nosi stroške izvedbe sam.

Dopolnilno vzdrževanje poteka do izteka pogodbe.

7. NADGRADNJE PORTALA IN VARNOSTNE SHEME MDDSZ

V času produkcijskega delovanja Portala MDDSZ lahko pride do večjih sprememb oz. dodatnih funkcionalnih zahtev glede Portala MDDSZ.

Cene posameznih nadgradenj bodo predmet posameznih povpraševanj na podlagi sklenjene pogodbe.

Naročnik v naslednjih dveh letih načrtuje naslednje dopolnitve oz. nadgradnje v okviru dopolnilnega vzdrževanja ter nadgradenj Portala in Varnostne sheme MDDSZ:

- optimizacija integracijskih logov na produkcijski Varnostni shemi,
- prenova produkcijskega, testnega ter zunanjega Portala MDDSZ,
- možnost vlaganja obrazcev za pridobitev pravic v IS MDDSZ v elektronski obliki.

7.1 Optimizacija integracijskih logov na produkcijski Varnostni shemi

Predvidena je izvedba optimizacije delovanja integracijskih postopkov med bazo Varnostne sheme in IS CSD.

7.2 Prenova produkcijskega, testnega ter zunanjega dela Portala MDDSZ

Predvidena je funkcionalna in oblikovna prenova Portala MDDSZ.

7.3 Možnost vlaganja obrazcev za pridobitev pravic v IS MDDSZ v elektronski obliki

Ministrstvo želi omogočiti bodočim uporabnikom oddajo e-vlog za pridobitev pravic dostopa do IS MDDSZ. E-vloge bodo omogočile zajem določenih podatkov in jih v predpisani obliki posredovale v Varnostno shemo.

Za oddajo e-vloge bo moral imeti uporabnik veljavno digitalno potrdilo ene od javnih certifikatnih agencij s katero bo vlogo tudi elektronsko podpisal. Vsaka e-vloge bo časovno žigosana, pri čemer je predvidena uporaba infrastrukture izdajatelja časovnih žigov na Ministrstvu za javno upravo.