eZapori-Projekt za izvedbo: Arhitektura, infrastruktura, upravljanje z informacijskimi tveganji

Osnovne lastnosti dokumenta

Opis in namen
Dokument za projekt IS eZapori opisuje infrastrukturo in topologijo storitev in gradnikov IS eZapori, prepoznava ključna informacijska tveganja in varnostne kontrole za njihovo obvladovanje. Opredeljuje ključna tveganja in nadzorne točke opredeljuje s področja regulativnih in infrastrukturnih tveganj.

Lastnost	Stanje
Naziv:	eZapori-Projekt za izvedbo: Arhitektura, infrastruktura, upravljanje z informacijskimi tveganji
Verzija:	1.1
Ime datoteke:	eZapori_PZI_A-I-UIT_v0.2
Status:	Neodobren
Datum izdelave:	20.08.2011
Izdelal:	Aleš Skubic, Rok Berdajs, Tomaž Degen, Luka Vrhovec, Andrej Nemanič, RRC d.d.
Datum pregleda:	
Pregledal:	
Datum odobritve:	
Odobril:	

Omejitve kroženja	Podjetje	Omejeno na
Dostop do in distribucija tega dokumenta je omejena s poslovnimi pravili podjetja RRC d.d.	Naročnik	Neomejeno
	Javnost	Polna omejenost
	Ostalo	Polna omejenost

Verzija	Datum	Avtor	Kratek opis
V-0.1	20.08.2011	A. Skubic	Izhodiščna verzija dokumenta; Arhitektura in infrastruktura
V-1.1	25.10.2011	RRC	Usklajena verzija

Kazalo vsebine

1 Uvod

Uprava RS za izvrševanje kazenskih sankcij (UIKS), ki je organ v sestavi Ministrstva za pravosodje, bo uporabnik informacijskega sistema eZapori, ki je predmet projekta. Zavodi za prestajanje kazni zapora in prevzgojni domovi so poleg Generalnega urada notranje organizacijske enote Uprave.

Naročnik, Uprava RS za izvrševanje kazenskih sankcij, je ocenil, da je najbolj optimalna rešitev informatizacije, da se kot osnovno ogrodje bodočega informacijskega sistema eZapori uporabi obstoječa platforma aplikacije iEZO, saj slednja uspešno pokriva nekaj temeljnih procesov Uprave in organov v sestavi. Zato je to tudi privzeto izhodišče za dograditve in dopolnitve.

Osrednji del IS eZapori predstavlja obstoječi informacijski sistem iEZO, ki bo dograjen:

- s procesi, (izvrševanjem kazni zapora, izvrševanjem mladoletniškega zapora, oddajanjem v prevzgojni dom, izvrševanjem uklonilnega zapora in izvrševanjem pripora) ki se izvajajo na ravni Zavoda in so/delno/niso informatiziran v sklopu informacijskega sistema iEZO, ki se dogradi in razširi z namenom da: se na enem mestu zbere vse podatke, ki so potrebni za namen obdelave osebnih podatkov, se omogoči obdelava zbranih podatkov po opredeljenih iskalnih parametrih, se omogoči prenos podatkov med različnimi organi javne uprave in zavodom.
- z evidencami in podatkovnimi zbirkami, ki izhajajo iz dodatne informatizacije
- s podatkovnimi integracijami z notranjimi (lastnimi) podatkovnimi zbirkami naročnika
- s podatkovnimi integracijami z zunanjimi (tujimi) podatkovnimi zbirkami, kot so: eZapori – Upravne Enote (UE), eZapori-CRP, eZapori-sodišče, Sodišče – eZapori, eZapori-CSD, eZapori - MNZ/Policija.

Arhitekturni in infrastrukturni del dokumenta podaja informacije o arhitekturni in tehnološki zasnovi IS eZapori, njegovih osnovnih gradnikih, njihovi medsebojni povezanosti in povezanosti na zunanje informacijske sisteme. Povzema informacije o razvojnem, testnem, referenčnem, uvajalnem in produkcijskem okolju naročnika.

Poleg zajema podatkov iz informacijskih sistemov zunanjih institucij bo IS eZapori igral pomembno vlogo pri posredovanju podatkov s področja obravnavane in zakonsko opredeljene vsebine vsem institucijam, ki imajo za to ustrezno zakonsko podlago.

Zato je potrebno pri načrtovanju in izvedbi informacijskega sistema upoštevati informacijska tveganja glede zaupnosti, celovitosti in razpoložljivosti ter posebno pozornost nameniti regulatornim in infrastrukturnim varnostnim tveganjem. Dokument identificira ključne grožnje, ki bi lahko na kakršenkoli način ogrozile varnost informacij, ki se bodo zajemale, združevale, obdelovale in izmenjavale znotraj IS eZapori.

Poseben poudarek je posvečen varstvu osebnih podatkov. Informacijski sistem namreč povezuje in hrani osebne podatke pridržanih oseb, kar predstavlja visoko informacijsko tveganje. Dokument podaja ključne zahteve glede informacijske varnosti in varstva teh podatkov, prepoznava ključna informacijska tveganja in podaja nadzorne mehanizme za njihovo učinkovito obvladovanje.

1.2 Referenčni dokumenti

Referenčni dokumenti predstavljajo osnovo za pripravo poglavja o infrastrukturi IS eZapori. Pričujoči dokument se na njih navezuje ali pa dodatno opisujejo zahteve za pripravo

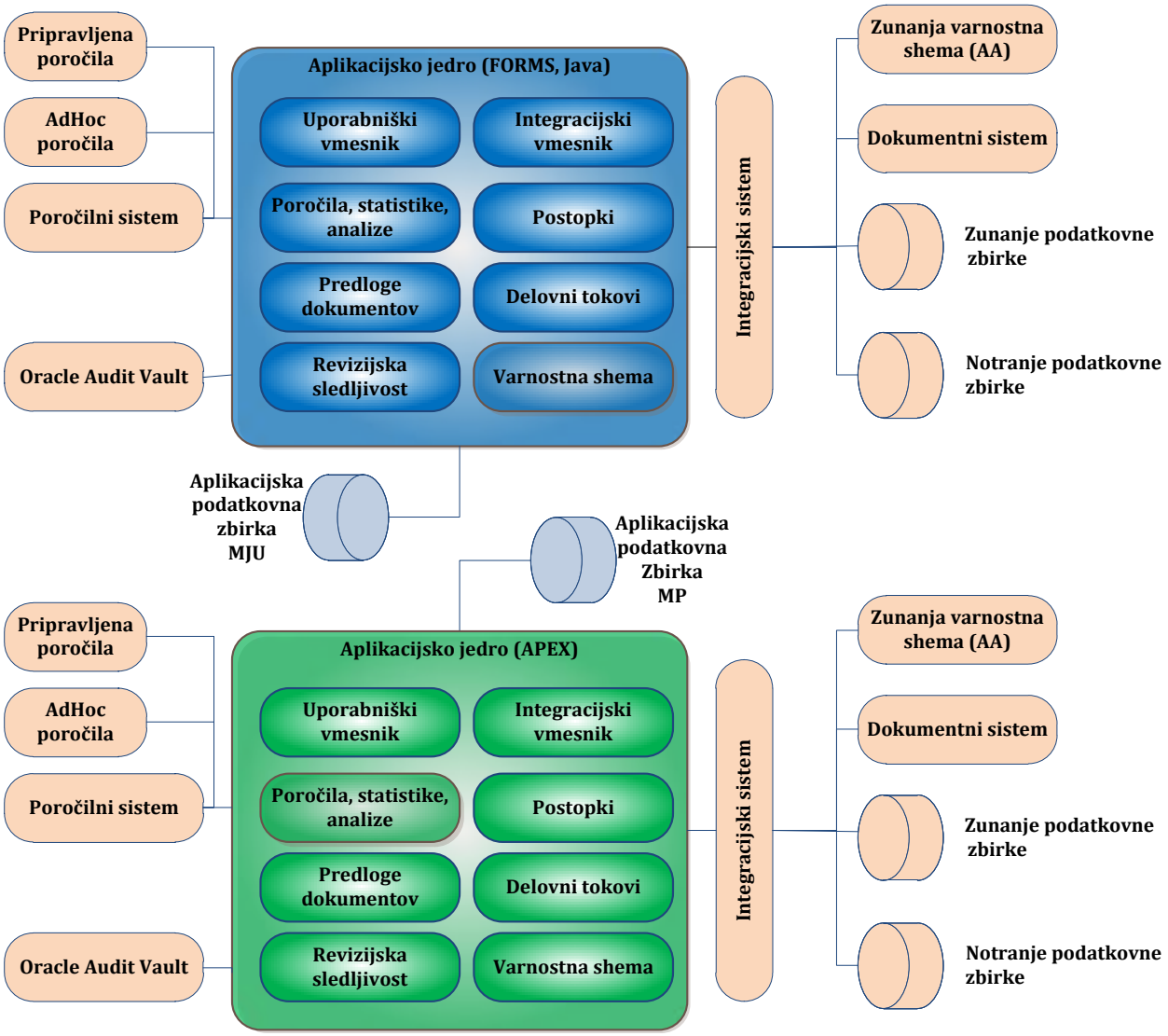
infrastrukturnega sklopa PZI. Vsi referenčni dokumenti ohranjajo lastno avtorsko in moralno pravico.

Ref.	Koda	Naslov in opis
[1]	Generične Tehnološke zahteve-v1.01.doc	vsebuje tehnološka izhodišča MJU
[2]	ci_mju.pdf	neprekinjena integracija MJU
[3]	MJU_SVN_Drevesna_Struktura_v0.10k.xls	Drevesna struktura odlagališča kode SVN na MJU
[4]	VOLRRE-tech_specs-v1.2.1-esb-sp	tehnične specifikacije referenčnega izvajalskega okolja JBOSS. Avtor: Grega Bremec, Virtualni odprtokodni laboratorij.
[5]	MJU-IntegracijaSOA.pdf	Dokument MJU, ki podaja vodila za izvedbo Integracije Oracle BPEL procesov prek JBoss ESB.
[6]	Navodila za obvladovanje sprememb preko SVNv02.doc	MJU/SCII/PDC Navodila Navodila za obvladovanje sprememb informacijskih sistemov preko SVN
[7]	Analiza-MJU-MP-v0.2	Analiza infrastrukture gostovanja IS MP in MJU
[8]	Analiza_procesi_v025.doc	eZapori - Krovna analiza procesov
[9]		Dokument arhitekture IS eZapori.
[10]	Smernice_za_razvoj_informacijskih_resitev.pdf	Smernice za razvoj informacijskih rešitev http://www.ip-rs.si/publikacije/prirocniki-in-smernice/
[11]	Analiza-MJU-MP-v1.0.docx	Analiza infrastrukture gostovanja IS MP in MJU
[12]	Oracle Application Express Best Practices, An Oracle White Paper January 2006	http://www.oracle.com/technetwork/testcontent/apex-best-practices-134310.pdf
[13]	Pro Oracle APEX	J.E. Scott, S. Spendolini: Pro Oracle Application Express (Apress, 2008),
[14]	Več naslovov	Tehnološka dokumentacija in navodila za povečanje varnosti znotraj APEX in FORMS. Referenčne vsebine so navedene znotraj besedila.

2 Arhitektura in infrastruktura sistema eZapori

2.1 Arhitekturna izhodišča

Arhitektura informacijskega sistema eZapori bo, glede na odločitev naročnika, porazdeljena. Večinski del modulov, vsebinsko in podatkovno tesno sklopljenih z obstoječim IS iEZO, bo tehnološko in infrastrukturno nameščen na infrastrukturi MJU, manjšinski del samostojnih modulov pa na infrastrukturi MP.



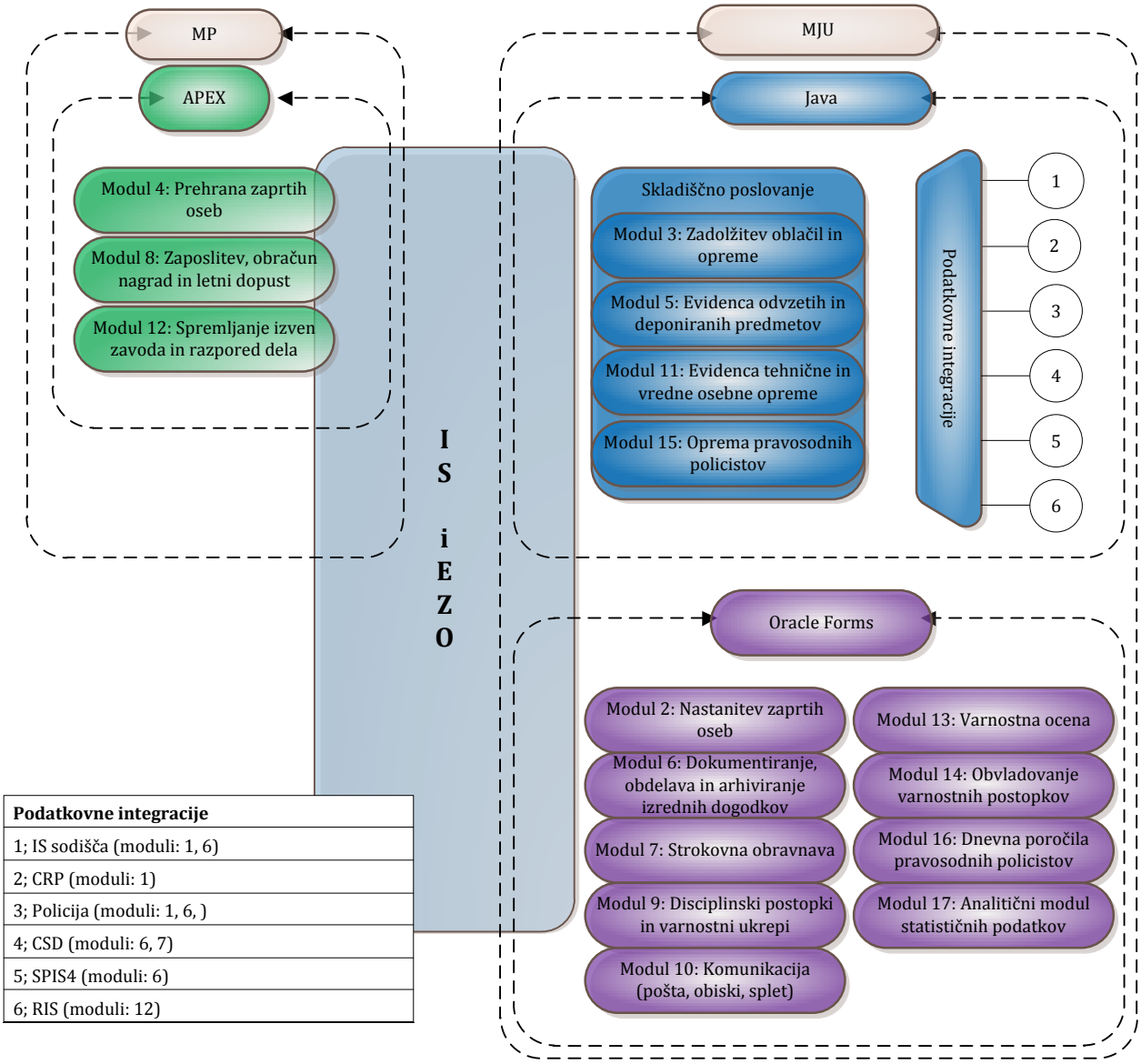
Slika 1: Arhitekturna slika sistema eZapori

Na arhitekturni shemi so generično označeni najznačilnejši gradniki zunanje, produkcijske (moduli IS eZapori) in obstoječe (Oracle in druge) infrastrukture naročnika, kot tudi zunanje (tretja stran) infrastrukture.
Porazdelitev modulov glede na predlagano tehnologijo in lokacijo gostovanja je prikazana v nadaljevanju.

Nov IS bo v polni meri izkoriščal:

- obstoječo in dograjeno Oracle informacijsko infrastrukturo MJU in MP (relacijsko bazo, Oracle BI Publisher za izdelavo naprednih poročil in izpisov in Oracle Audit Vault za napredno in celovito izvedbo revizijske sledljivosti skladne z ZVOP (tudi vpogledi);
- drugo informacijsko infrastrukturo naročnika (varnostna območja MJU, Apache spletne strežnike, infrastrukturo poročanja in priprave poročil (Oracle Discoverer), dokumentni sistem SPIS, servis elektronske pošte);
- drugo zunanjo informacijsko infrastrukturo (javni sistemi CA);

ter dodajal produkcijsko infrastrukturo storitve, ki jih mora zagotoviti nov IS.



Podatkovne integracije
1; IS sodišča (moduli: 1, 6)
2; CRP (moduli: 1)
3; Policija (moduli: 1, 6,)
4; CSD (moduli: 6, 7)
5; SPIS4 (moduli: 6)
6; RIS (moduli: 12)

Slika 2; Moduli IS eZapori, tehnologija in izvajalno okolje

2.1.1 Arhitektura razvojnih okolij

2.1.1.1 Arhitektura Oracle FORMS 11g

Oracle FORMS okolje sestavljata razvojno in izvajalno okolje. Oracle Forms Developer je razvojno orodje za poslovne spletne aplikacije, ki so namenjene procesiranju velikih količin podatkov, kompleksnih izračunov, analiz in transakcij. Oracle Forms zagotavljajo odprti in razširljiv model, ki omogoča popolno kostumizacijo in razširitev aplikacije z Javo.

Oracle Fusion Middleware Forms Services je aplikacijski strežnik z ustreznimi servisi, ki so optimizirani za namestitev Oracle Forms aplikacij na splet. Servisi zagotavljajo upravljanje transakcij, zaklepanje zapisov, predpomnenje in upravljanje z napakami.

Oracle Forms Developer in Oracle Forms Services zagotavljata celovito aplikacijsko ogrodje za optimalni razvoj, testiranje in namestitev Oracle Forms aplikacij tako na internetu, kot na lokalnih

omrežjih. Skupaj nam dajeta okolje za hiter razvoj aplikacij (RAD), ki je odprto, nadgradljivo in omogoča:

- prenos obstoječe aplikacije v skladu z novimi tehnološkimi smernicami,
- enostavno razširitev uporabniškega vmesnika z Java komponentami,
- uporabo in integracijo Java in XML tehnologij.

Oracle Fusion Middleware Forms Services – Arhitektura

Oracle Fusion Middleware Forms Services sestavljajo tri komponente: Forms odjemalec, ki se avtomatično naloži v spletnem brskalniku končnega uporabnika, strežniški program Forms Listener Servlet in Forms Runtime izvajalno okolje na aplikacijskem strežniku.

Forms odjemalec

Ko uporabnik zažene Forms sejo, se odjemalec (Java applet), dinamično naloži iz Oracle Fusion Middleware aplikacijskega strežnika. Ta generični applet zagotovi uporabniški vmesnik za Forms Runtime proces, ki se izvaja na aplikacijskem strežniku. Zagotovi uporabniško interakcijo in vizualni odziv, kot je npr. navigacija med polji forme ali pa klik na določen gumb. Isti Java applet se uporabi za vse Forms aplikacije in se zato naloži samo enkrat.

Predpogoj za izvajanje Java appleta v spletnem brskalniku je Java Virtual Machine (JVM), ki je nameščen na lokalnem računalniku. JVM je odvisen od platforme na kateri deluje, Oracle pa priporoča Sun 1.6 JRE za Oracle Forms 11g.

Forms Runtime Process

Forms Runtime Process je proces, ki vzdržuje povezavo do podatkovne baze v imenu Forms klienta. Proces se kreira ob uporabnikovem dostopu do strani s Forms aplikacijo. Prav tako pa se proces tudi avtomatsko zaključi čim uporabnik zapre aplikacijo oziroma svoj spletni brskalnik.

Forms Listener Servlet

Forms Listener strežniški program:

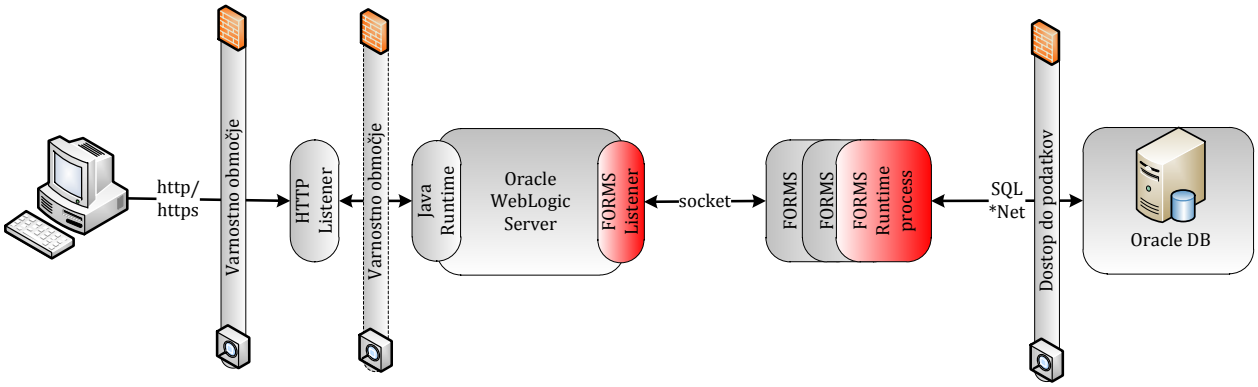
- kreira Forms Runtime proces za vsakega klienta ob dostopu uporabnika do aplikacije,
- zapre Runtime proces ob uporabnikovem izhodu iz aplikacije,
- izvaja mrežno komunikacijo med klientom in Runtime procesom.

Proces povezovanja

Znotraj Oracle Fusion Middleware Forms Services arhitekture obstaja samo ena povezava med odjemalcem in HTTP Listener, podobno kot v vsaki spletni aplikaciji. HTTP Listener usmerja zahteve do Forms Listener Servleta, ki upravlja zahteve od Forms odjemalca do Forms Runtime.

Komunikacija vedno poteka skozi HTTP Listener, tako da ima aplikacija samo en odprti port do interneta. Modularni gradniki omogočajo več točk nadzora in upravljanja prometa, prav tako pa uporabo vseh vrst posrednikov (proxy) in delilnikov prometa (balancer) na več ravneh.

Po tem scenariju pošlje klient HTTP zahtevo in prejme HTTP odgovor od HTTP Listener procesa. Ker HTTP Listener za klienta izgleda kot mrežna končna točka, ostali strežniški naslovi in vrata (port) niso odprti navzven, kar je prikazano v spodnji sliki:



Slika 3: Oracle FORMS arhitektura

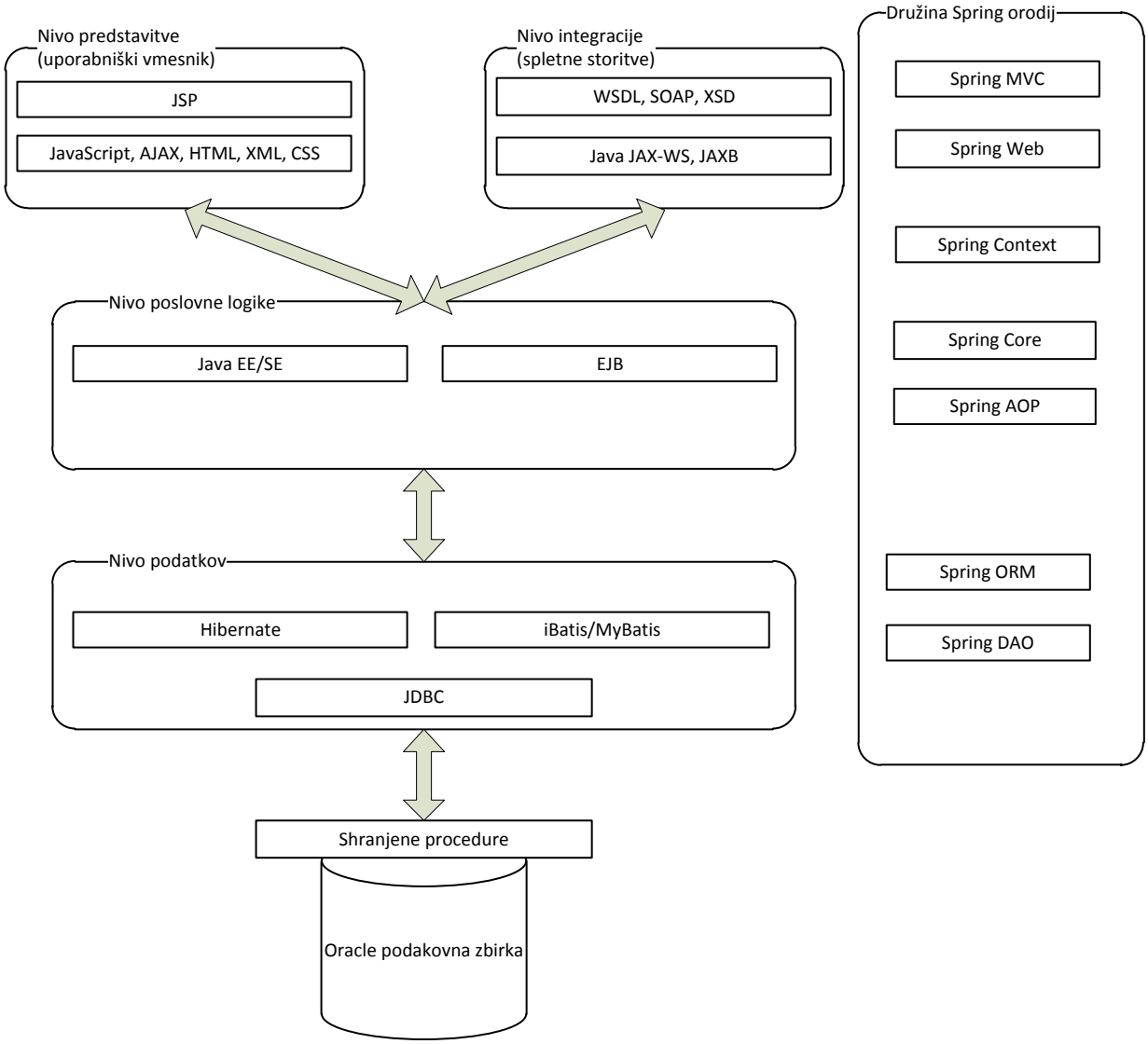
2.1.1.2 Arhitektura Java

Java del aplikacije je razdeljen na več nivojev. Logično so razdeljeni na nivo podatkov, nivo poslovne logike ter nivo predstavitve ali nivo integracije.

Kot osnovna je uporabljena družina Spring ogrodij, s katerim pokrijemo večino zgoraj navedenih nivojev. Dodatno za nivoje uporabljamo še:

- nivo podatkov: ogrodji Hibernate ali iBatis/MyBatis
- nivo poslovne logike: Java EE ali Java SE. Za dodatno modularnost poslovne logike EJB
- nivo predstavitve: JSP, JavaScript, AJAX, HTML, XML, CSS, uporaba vzorca MVC (angl. Model-View-Controller)
- nivo integracije: uporaba Java ogrodij JAX-WS, JAXB, WSDL, XSD, SOAP

Ogrodje za izgradnjo (angl. build) je MAVEN. Za testiranje posameznih metod (angl. unit testing) uporabljamo ogrodje testNG. Performačno testiranje izvajamo z uporabo orodja JMeter.



Slika 4: Logični nivoji Java dela aplikacije ter uporabljene tehnologije, programski jeziki ter notacije

2.1.1.3 Arhitektura Oracle APEX

Oracle Application Express (Oracle APEX) je brezplačno, spletno razvojno orodje, ki omogoča hiter razvoj varnih, zanesljivih in visoko razpoložljivih spletnih rešitev v povezavi z Oracle relacijsko bazo. Oracle Application Express je certificirano podprt za vse izdaje Oracle Database 11g vključno z Enterprise Edition (ki omogoča implementacijo še dodatnih varnostnih funkcionalnosti).

Oracle Application Express je mogoče namestiti kot del namestitve podatkovne zbirke z Oracle Database 11gR2 (za naročnikov primer). Pri razvoju določenih modulov IS eZapori bomo uporabili trenutno zadnjo razpoložljivo verzijo APEX 4.1.

Oracle Application Express sestavlja skladišče metapodatkov, ki shranjuje opredelitve vlog in stroja (Application Express engine), ki gradi in procesira spletne strani. Je v celoti integriran v podatkovno zbirko Oracle. Ključni gradnik APEX so podatki v tabelah in velika količina preverjene in varne PL / SQL kode. Bistvo Oracle Application Express je približno 425 tabel in 230 PL / SQL paketov, ki vsebujejo več kot 425.000 vrstic kode.

Ključne naloge APEX stroja so:

- Upravljanje seje (Session state management),
- Storitve razpoznavanja (Authentication Services),
- Storitve avtorizacije (Authorization Services),
- nadzor pretoka strani (Page Flow Control),
- procesiranje potrditev (Validation Processing),
- Izgradnja in obdelava strani (Rendering and Page Processing)

Arhitektura asinhronega nadzora stanja seje zagotavlja minimalno izrabo CPU virov. Brskalnik pošlje URL zahtevo, ki se prevede v ustrezni Oracle Application Express PL/SQL klic. Po opravljenem procesiranju PL/SQL zahtevka znotraj relacijske baze, je odgovor (rezultat) vrnjen brskalniku v obliki HTML. Ta ciklus se zgodi ob vsaki zahtevi ali predaji zahtevka ali strani. Stanje vsake trenutne seje je upravljano znotraj relacijske baze in ne uporablja namenske bazne povezave. Vsak vpogled povzroči novo bazno sejo, zato so viri relacijske baze uporabljeni le, ko Application Express stroj procesira zahtevek ali gradi stran.

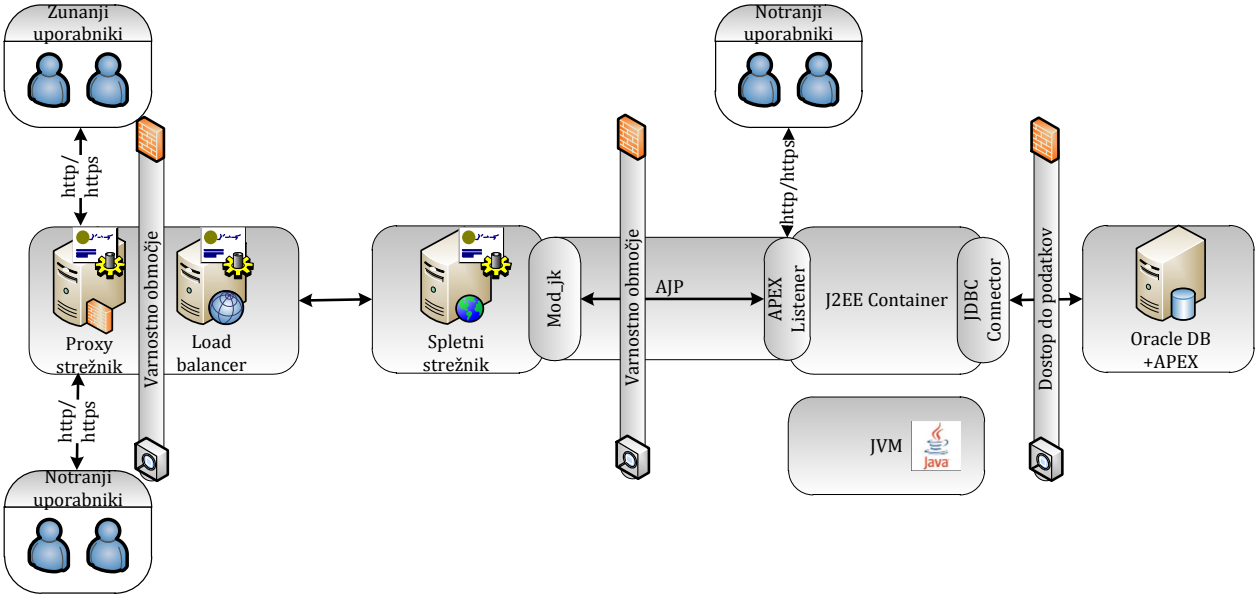
Application Express stroj je dostopen iz spletnega brskalnika le preko spletnega strežnika. Aplikacijo gradi v realnem času iz skladišča metapodatkov, ki so hranjeni v tabelah zbirke podatkov. Gradnja ali razširitev aplikacije ne povzroči generacije dodatne kode, ki bodo nastajali, namesto tega so zgrajeni ali spremenjeni le metapodatki znotraj relacijske baze.

Za dostop odjemalca do spletnega strežnika so možni trije scenariji, vendar v nadaljevanju navajamo le napredno konfiguracijo, ki izpolnjuje vse naročnikove varnostne, zanesljivostne in druge kriterije in je sprejemljiva glede na obstoječo naročnikovo infrastrukturo in dodatne zahteve, opredeljene v dokumentu Tehnične specifikacije. To je izvedba razširjene konfiguracije Application Express poslušalca (APEX Listener).

Nov Oracle APEX Listener je na J2EE arhitekturi temelječa alternativa za Oracle HTTP Server (OHS) in mod_plsql. J2EE implementacija ponuja izjemno povečanje funkcionalnosti, vključno s: spletno konfiguracijo, izboljšano varnostjo in predhrambo datotek (file caching).
APEX Listener zagotavlja prilagodljivost s certificirano podporo uporabi Oracle Web Logic Server, ki bo uporabljen v tem primeru.

Oracle Application Express arhitektura zahteva neko obliko spletnega strežnika, kot posrednika zahtev med spletnim brskalnikom in Oracle Application Express strojem. APEX Listener je bil ustvarjen, da izpolnjuje in presega to zahtevo. Uporaba Oracle APEX Listener z uporabo vgrajenih JDBC gonilnikov močno poenostavlja proces razvoja in širitve aplikacije.

Za rešitve, ki delujejo izven lokalnega (intranetnega) okolja, ali rešitve v gostujočem okolju je pomembno, da sta Oracle APEX in HTTP poslušalec (listener) nameščen vsak na svoji strani požarnega zidu. Prvi na notranji, varni strani in drugi na zunanji, javni strani. Zahteve od odjemalca do strežnika potujejo preko zunanjega spletnega strežnika, skozi požarni zid (in druge morebitne nameščene sisteme: Proxy strežniki, Load Balancer strežniki, ipd) preko APEX Listener-ja do APEX stroja. Takšna konfiguracija je predvidena tudi v primeru APEX modulov IS eZapori v gostovalni domeni Ministrstva za pravosodje.



Slika 5; Oracle APEX arhitektura

Posebna prednost rešitve, ki jo ponuja APEX Listener znotraj J2EE vsebnika (kontejnerja) pa je možnost neposredne integracije z JVM, kar omogoča transparentno sobivanje obeh arhitektur ter optimalni izkoristek prednosti obeh. Podrobnejše informacije so na voljo na:

- http://www.oracle.com/technology/products/database/application_express/apex_listener/apex_listener.html
- http://www.oracle.com/technology/products/database/application_express/index.html

2.2 Arhitekturne ravni IS

Pri načrtovanju rešitve je imel izvajalec v mislih osnovne zahteve moderne gradnje informacijskih sistemov, kot so: zanesljivost, širljivost, prilagodljivost, varnost in povezljivost. Predlagana rešitev je z navedenimi vodili skladna v vseh stopnjah svojega razvoja.

Arhitektura je več nivojska. Osnovni arhitekturni gradniki rešitve so:

- **podatkovna baza**, ki se uporablja za varno hrambo in dostop do vseh podatkov, revizijsko sledenje ipd.
- **podatkovna izmenjava**, ki skrbi za varno, nadzorovano izmenjavo podatkov s šibko sklopljenimi zunanjimi podatkovnimi zbirkami. Pretok podatkov bo izveden s pomočjo eno ali dvosmernega vmesnika (odvisno od tipa podatkovne izmenjave) na vseh šibko sklopljenih informacijskih sistemih.
- **poslovna logika**, ki nadgrajuje podatkovno hrambo s postopki podatkovne integracije in implementiranimi poslovnimi pravili. Cilj je izvesti čim več rešitev na standardizirani osnovi.
- **raven uporabniškega vmesnika**, ki poskrbi za podatkovni zajem in osnovno validacijo.

2.2.1 Raven podatkovnega dostopa in hrambe

Raven podatkovnega dostopa skrbi za prenos podatkov poslovnega in sloja izmenjave podatkov do podatkovnega strežnika, ki hrani podatke, centralne šifrante in meta podatke. Glede na definirana poslovna pravila skrbi za integriteto podatkov in vsebuje proceduralne postopke/obdelave nad hranjenimi podatki.

Poudarek predlagane rešitve IS eZapori je skrb za podatke, varnost in revizijska sledljivost!

Pomembna funkcionalnost ravni je implementacija vertikalne in horizontalne varnostne politike ter hranjenje revizijske sledi dostopa do podatkov. Z združenjem naštetih funkcionalnosti je na enostaven, kontroliran in učinkovit način, preko različnih medijev (npr. uporabniške maske, prenosi podatkov preko standardiziranih protokolov, uvoz podatkov preko zunanjega vmesnika...), zagotovljen dostop do podatkov.

Razvojno, testno in produkcijsko (RTP) okolje podatkovnega dostopa in hrambe MJU in izvajalca predstavlja Oracle Database 11g Enterprise Edition, Release 11.2.0.2.0 - 64bit. Podrobnejši podatki so:

Raven podatkovnega dostopa in hrambe – okolje MJU	
Relacijska baza	Oracle Database 11g Enterprise Edition Release 11.2.0.2.0 - 64bit
PL/SQL Release	11.2.0.2.0-Production
CORE	11.2.0.2.0-Production
TNS for Linux	11.2.0.2.0-Production
NLSRTL Version	11.2.0.2.0-Production
NLS_CHARACTERSET	AL32UTF8
NLS_LENGTH_SEMANTICS	CHAR
NLS_NCHAR_CHARACTERSET	AL16UTF16
NLS_RDBMS_VERSION	11.2.0.2.0
Operacijski sistemi	SUSE Linux-64 bit, OEL v5-64 bit
Virtualizacija	VMWare, Oracle VM

Razvojno, testno in produkcijsko (RTP) okolje podatkovnega dostopa in hrambe MP predstavlja Oracle Database 11g Enterprise Edition, Release 11.2.0.1.0 - 64bit. Podrobnejši podatki so:

Raven podatkovnega dostopa in hrambe – okolje MP	
Relacijska baza	Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit
PL/SQL Release	11.2.0.1.0-Production
CORE	11.2.0.1.0-Production
TNS for Linux	11.2.0.1.0-Production
NLSRTL Version	11.2.0.1.0-Production
NLS_CHARACTERSET	AL32UTF8
NLS_LENGTH_SEMANTICS	BYTE
NLS_NCHAR_CHARACTERSET	AL16UTF16
NLS_RDBMS_VERSION	11.2.0.1.0
Operacijski sistemi	OEL v5-64 bit
Virtualizacija	Oracle VM

2.2.2 Gradniki podatkovne izmenjave

Informacijski sistem bo za komunikacijo v okviru posameznega homogenega sklopa uporabljal vmesnike na aplikativnem nivoju. Povezovanje z ostalimi podsistemi in zunanjimi viri podatkov bo praviloma izvedeno s pomočjo standardiziranih spletnih storitev. V primeru povezovanja z obstoječimi informacijskimi sistemi, namenske opreme in orodij pa preko izmenjave, ki jih obstoječi sistemi podpirajo (»Database Link«, tekstovne datoteke,…).

Za povezave na zunanje podatkovne zbirke kot tudi objavo spletnih servisov IS eZapori je naročnik predvidel izvedbo, skladno z dokumentom [5]. Dokument kratko opisuje infrastrukturo, ki podpira moderno arhitekturo spletnih storitev znotraj Ministrstva za javno upravo, ter način kako pripraviti poslovne procese za možnost ponovne uporabe v drugih programskih modulih in procesih.
Testno okolje, ki ga predstavljajo: zunanji izvajalni objekti (viewlets) in virtualizirani SOA strežnik je izvajalec prevzel na MJU-DEUP in predstavlja del njegovega R-T okolja.

Kot referenčni aplikacijski strežnik za podatkovno integracijo je predviden JBoss 5.1 z implementirano naravno (native) podporo za JAX-WS/JAXB (2.2) spletne storitve.

Izdelava ter testiranje spletnih storitev kot jih definira specifikacija JSR-181-Web Services Metadata for the JavaTM Platform, je v Java EE enostavno in hitro zaradi uporabe pripomb (anotacij) za opis metapodatkov spletne storitve, ki jih dodamo v izvorno kodo, s katero implementiramo spletno storitev. Opisano predstavlja tudi bistveno prednost izbire v primerjavi s specifikacijo JSR-109-Implementing Enterprise Web Services. Podpora spletnim storitvam v Java EE temelji na JAX-WS (Java API for XML Web Services) in JAXB (Java API for XML Binding) APIjih, ter podpori za metapodatke.

Pri izmenjavi velikih količin podatkov med podsistemi(npr. sinhronizacija z zunanjimi šifranti, prenos rezultatov obdelave, obsežni izpisi) izvajalec predlaga paketni prenos podatkov preko definiranih vmesnikov.

Podatkovna izmenjava MJU – Referenčno okolje	
Aplikacijski strežnik	JBoss 5.1 JAX-WS (2.2) support,
Dodatna programska oprema	JBoss Application Server 5 (JavaEE 5 compliant) web service stack EJB 2.1, EJB3 and JSE endpoints, Attachments Profile Version 1.0, Support for MTOM/XOP and SwA-Ref, WS-Security 1.0 for XML Encryption/Signature of the SOAP message, WS-Addressing (W3C candidate release) and JSR-261 WS-ReliableMessaging, WS-Eventing, WS-Policy
Virtualizacija	VMWare ali Oracle VM
Operacijski sistemi	SUSE Linux, 64 bit ali OEL v5, 64 bit

Podrobnejši opis, kot tudi arhitekturno izbiro integracijskih skladov opisuje dokumentacija na spletni strani: http://www.jboss.org/jbossws.

Podatkovna izmenjava - MJU	
Aplikacijski strežnik	WebLogic 11gR1 (10.3.3)
Javansko okolje	Java JRockit (jdk1.6.0_20-R28.1.0-4.0.1)
Operacijski sistemi	SUSE Linux, 64 bit ali OEL v5, 64 bit
Virtualizacija	VMWare ali Oracle VM

Podatkovna izmenjava - MP	
Aplikacijski strežnik	Oracle WebLogic 11gR1 (10.3.2),

Javansko izvajalno okolje	Java JRockit (jdk1.6.0_20-R28.1.0-4.0.1)
Virtualizacija	Oracle VM
Operacijski sistemi	OEL v5, 64 bit

2.2.3 Integracija z zunanjimi podatkovnimi zbirkami

2.2.4 Poslovna raven

Poslovna raven, preko aplikacijskega strežnika, implementira večino poslovne logike, ki je zajeta v aplikaciji. Glede na definirana poslovna pravila skrbi za integriteto podatkov in vsebuje proceduralne postopke/obdelave nad hranjenimi podatki. Zahtevane funkcionalnosti so navzven predstavljene preko spletnih storitev, ki so namenjene odjemalski aplikaciji. Določene integracijske točke z zalednimi sistemi so predvidene na ravni aplikacijskega strežnika.

Poslovna raven – Javansko izvajalno okolje MJU	
Aplikacijski strežnik	WebLogic 11gR1 (10.3.3)
Javansko okolje	Java JRockit (jdk1.6.0_20-R28.1.0-4.0.1)
Operacijski sistemi	SUSE Linux, 64 bit ali OEL v5, 64 bit
Virtualizacija	VMWare ali Oracle VM

Poslovna raven – Oracle Forms izvajalno okolje MJU (podatki v času oddaje niso dostopni)	
Aplikacijski strežnik	WebLogic 11gR1 (10.3.3)
Forms okolje	Forms Runtime Process: Forms Listener Servlet: Weblogic Java Runtime: http Listener:
Operacijski sistemi	SUSE Linux, 64 bit ali OEL v5, 64 bit
Virtualizacija	VMWare ali Oracle VM

2.2.5 Predstavitvena raven (javansko izvajalno okolje)

Uporabniški vmesnik bo implementiran kot spletna aplikacija. Ključni modul IS eZapori iEZO je bil razvit z izključno zahtevo po podpori brskalnikov družine MS Internet Explorer. Ker prenova iEZO v tej fazi razvoja še ni predvidena, je za kakovostno uporabo celotnega IS predlagana izbira Internet Explorer spletnega brskalnika.

Uporabniški vmesnik bo zgrajen tako, da končnim uporabnikom čim bolj olajša uporabo aplikacije: jasno in intuitivno, nazivi (labele) in grafični elementi so skladni skozi celotni informacijski sistem, povsod, kjer je to mogoče in dovoljeno s ciljem olajšanja vnosa podatkov, uporabniku ponudi privzete vrednosti; v primerih napačnih vnosov in/ali napake je uporabnik o napaki obveščen s poudarjenim sporočilom (pop-up message).

	*Med WebLogic produkcijskimi strežniki je potrebno vzpostaviti replikacijo med http sejami (http Session Replication), ki bodo zagotovile, da se spremembe znotraj JVM propagirajo znotraj vseh WebLogic strežnikov.*

R-T-P javanskega izvajalnega okolja predstavlja osnovo za uspešno integracijsko in uporabniško testiranje uporabniškega okolja. Določeno je v referenčnem dokumentu [1] in predstavlja osnovno R-T okolje izvajalca.

Predstavitvena raven - MJU	
Aplikacijski strežnik	WebLogic 11gR1 (10.3.3)
Javansko okolje	Java JRockit (jdk1.6.0_20-R28.1.0-4.0.1)
Operacijski sistemi	SUSE Linux, 64 bit ali OEL v5, 64 bit
Virtualizacija	VMWare ali Oracle VM

Predstavitvena raven - MP	
Aplikacijski strežnik	Oracle WebLogic 11gR1 (10.3.2),
Javansko okolje	Java JRockit (jdk1.6.0_20-R28.1.0-4.0.1)
Dodatna programska oprema	
Operacijski sistemi	Oracle VM
Virtualizacija	OEL v5, 64 bit

2.2.6 Izpisi in poročila

Obstoječi IS iEZO za izpis poročil uporablja orodje Oracle Reports. S tem namenom se bo večina poročil novega IS eZapori pripravila z enakim orodjem. Za analitična in AdHoc poročila se predvideva uporaba orodja Oracle Discoverer in/ali Oracle Application Express.
Več informacij o posameznem orodju je dostopnih na:
http://www.oracle.com/technetwork/middleware/reports/overview/index.html
http://www.oracle.com/technetwork/developer-tools/discoverer/overview/index.html
http://apex.oracle.com/i/index.html

Predstavitvena raven	
Aplikacijski strežnik	WebLogic 11gR1 (10.3.3)
Dodatna programska oprema	Oracle Discoverer (11.1.1.2) JasperSoft Business Intelligence Suite
Operacijski sistemi	SUSE Linux, 64 bit ali OEL v5, 64 bit
Virtualizacija	VMWare ali Oracle VM

2.3 Varnostna shema in prepoznavanje

Varnostna shema zagotavlja**:** upravljanje in administracijo uporabnikov in njihovih vlog na posameznih aplikacijah ter upravljanje in administracijo storitev in storitvenih vlog na posameznih integracijskih točkah.

2.3.1 Upravljanje in administracija

V podrobnejši vsebini in specifikaciji je posebna pozornost namenjena poslovnemu pogledu na upravljanje uporabniškega dostopa. Le-ta vsebuje: uporabniško registracijo, upravljanje pravic, upravljanje uporabniških gesel in urejanje ter pregled pravic dostopa.

Modul za upravljanje in administracijo je namenjen nadzorovanemu dodajanju uporabniških pravil in pooblastil, preverjanju in posodabljanju teh pooblastil. Upravljavski modul je kot osrednji administrativni in upravljavski modul povezan z vsemi gradniki celovitega IS eZapori. Vsi dogodki se beležijo v središčnem nadzornem (audit) modulu, tako da je zagotovljena polna revizijska sledljivost. Informacijska rešitev bo podpirala upravljanje z uporabniki po sistemu vlog (Role Based Security). Posebna, administrativna vloga je skrbnik sistema, ki upravlja uporabniške pravice in dostope.

Načrtovana varnostna funkcionalnost omogoča model varnostne sheme, ki zagotavlja, da prijavljeni uporabnik na spletni maski lahko izvaja (vidi) samo tiste akcije, ki jih določi vloga ter da je vsako sejno zrno (poslovna logika sistema) zavarovano tako, da je klic metode onemogočen, če pred klicem metode ni narejena prijava s pripadajočo vlogo. Sistem razporejenih uporabniških vlog in dostopov odpravlja pomanjkljivosti na področjih:

- Standardni profili dostopa za uporabnike,
- Uporaba unikatnih uporabniških identifikatorjev,
- Uporaba drugačnih identifikatorjev za upravljavce sistema,
- Shranjevanje gesel v nezaščiteni obliki,
- Privzeta gesla naprav in sistemov.

Tipični dogodki, ki se zgodijo v življenjskem ciklu povezave uporabnika in/ali storitve znotraj informacijskega sistema so:

- Registracija uporabnika/storitve,
- Kreiranje računa (zagotovitev digitalne identitete),
- Sprememba gesla,
- Spreminjanje podatkov o uporabniku,
- Dodajanje in odvzemanje pravic dostopa,
- Brisanje računa.

2.3.1.1 Registracija uporabnika/storitve

Registracijo uporabnika/storitve izvaja skrbnik aplikacije, skladno z lastnimi poslovnimi pravili.

2.3.1.2 Kreiranje računa

Uporabnike kreira skrbnik aplikacije. Določi uporabniško ime, vlogo in dvakrat vnese geslo (potrditev pravilnosti).

2.3.1.3 Sprememba gesla

Vsak uporabnik ima pravico spremenit svoje geslo. Uporabniško ime ni mogoče izbirati ali dodajati. V kolikor se geslo pozabi, ga tudi skrbnik aplikacije ne more spremeniti.

2.3.1.4 Spreminjanje podatkov o uporabniku

Skrbnik aplikacije lahko po potrebni spremeni podatke o uporabniku:

- Spremeni zavod zaposlenega/servisa
- Spremeni ime in priimek/opis
- Spremeni podatke o podpisu in delovnem mestu
- Spremeni vlogo – rolo. Ko se vloga spremeni se vse pravice umaknejo in na novo ustrezno dodelijo (revoke vseh pravic in ponovno grant novih pravic)

2.3.1.5 Dodajanje in odvzemanje pravic dostopa

Dodajanje in odvzemanje pravic dostopa izvaja skrbnik aplikacije, skladno z lastnimi poslovnimi pravili.

2.3.1.6 Brisanje računa

Namesto brisanja računa se uporabi funkcija deaktivacije (stanje neaktivnosti). Vsak uporabnik ali storitev ima znotraj IS naveden podatek o pogoju veljavnega dostopa (zaposlitev, ipd). Ko uporabnik ni več zaposlen, se mu odstranijo pravice, ko podatkovna integracija ni več potrebna se ukine dostop.

2.3.2 Koncept uporabniških računov

Uporaba eZapori bo dovoljena le registriranim in v postopku uporabniškega razpoznavanja (avtentikacije) uspešno razpoznanim uporabnikom.

Vsakemu uporabniku bo omogočen dostop do posamičnih operativnih celot v eZapori v skladu z uporabniško skupino, ki ji pripada. Operativne celote predstavljajo posamezne funkcionalne sklope eZapori. Podrobnosti glede vlog in njihovega dostopa do posameznih operativnih celot bodo usklajene naknadno (po opravljeni podrobnejši analizi).

2.3.2.1 Uporabniške vloge

Aplikacija iEZO uporablja bazne uporabnike, ki imajo pravice omejene z baznimi vlogami in znotraj aplikacije. Uporabniško ime se uporablja tudi za uporabo orodja Oracle Discoverer. Za uporabo so trenutno v uporabi tri role, z različnimi pravicami:

- R_EZO_ADMINISTRATOR
- R_EZO_REFERENT
- R_EZO_UPORABNIK

Uporabnike lahko kreira samo administrator (uporabnik z rolo R_EZO_ADMINISTRATOR). Geslo lahko spreminja vsak uporabnik sam. Brisanje uporabnikov ni omogočeno.

Vse uporabniške vloge, kot tudi sistemski uporabniški računi bodo poimenovani po vzorcu: R_eZapori_vloga. Njihovo upravljanje se izvaja preko osrednjega administracijskega modula s posebnimi varnostnimi zahtevami.

Za izvedbo določenih operacij nad podatki visokega razreda varnostnih zahtev, oziroma za administracijo sistema, bo eZapori poleg razpoznavanja z uporabniškim imenom in geslom (ob vstopu v eZapori) od uporabnika zahteval tudi uporabo digitalnega potrdila. Takšne operacije so:

- Administracija uporabnikov in uporabniških vlog; dostop je omejen za uporabnike s SIGOV.CA certifikati,
- Vloge, ki vnašajo osebne podatke oz. podatke o kazni (IK Referenti); dostop je omejen za uporabnike s SIGOV.CA certifikati.

Uporabniki so hkrati bazni in aplikacijski. Baznemu uporabniku se dodeli ustrezna vloga, ki ima vse potrebne pravice. Pravice za kreiranje uporabnika in dodeljevanje baznih vlog ima samo uporabnik EZO, ki je nosilec vse programske kode in podatkov. Bazni uporabnik EZO je zaklenjen in se ne uporablja.

Pravice, ki jih ima uporabnik EZO v povezavi s kreiranjem uporabnikov:

- grant create session to ezo with admin option
- grant create user to ezo
- grant drop user to ezo
- grant r_ezo_administrator to ezo with admin option
- grant r_ezo_referent to ezo with admin option
- grant r_ezo_uporabnik to ezo with admin option.

R_EZO_ADMINISTRATOR; Vloga ima pravico insert, update, delete in select na vse tabele v shemi EZO. Vloga ima pravico uporabljati Oracle Discoverer, kjer lahko pripravlja - popravlja

poročila, jih shranjuje in dodeljuje ostalim uporabnikom. Vloga ima pravico izvajati procedure za ažuriranje uporabnikov. To rolo bodo uporabljali le skrbniki aplikacije, ki lahko pregledujejo in spreminjajo vse podatke.

R_EZO_REFERENT; Vloga ima pravico insert, update, delete in select na vse tabele v shemi EZO. Izjema so tabele s šifranti, parametri in z zgodovino, kjer ima vloga samo pravico select. Vloga ima pravico uporabljati Oracle Discoverer, kjer lahko pregleduje poročila, jih shranjuje in dodeljuje ostalim uporabnikom. To vlogo bodo uporabljali referenti v IK pisarni. **R_EZO_UPORABNIK**; Vloga ima pravico insert select na vse tabele v shemi EZO. Vloga ima pravico uporabljati Oracle Discoverer, kjer lahko pregleduje poročila. To rolo bodo uporabljali ostali sodelujoči v modulu iEZO.

V nadaljnjem razvoju IS eZapori je predvideno po trenutni oceni ca 20 novih vlog, med njimi različne uporabniške, administrativne, vloge za različne module, spletne storitve, podatkovno integracijo in druge. Njihova specifikacija bo jasna po zaključeni podrobnejši vsebinski analizi posameznega modula.

2.3.3 Koncept storitvenih računov

Uporaba spletnih storitev eZapori bo dovoljena le registriranim in v postopku razpoznavanja (avtentikacije) uspešno razpoznanim integracijskim storitvam (spletnim servisom).

2.3.4 Avtorizacija (uporabniki in storitve)

2.3.4.1 Prepoznavanje uporabnikov

Prepoznavanja uporabnikov poteka glede na dodeljeno uporabniško ime in geslo, ki skupaj tvorita uporabniško digitalno identiteto.

Ob prijavi v IS eZapori uporabnik vnese podatke o svoji digitalni identiteti. Privzeta avtorizacija za uporabnika je njej nadrejena avtorizacija uporabnikove vloge. Vsaka sprememba avtorizacije na nivoju vloge se odrazi tudi na avtorizaciji za uporabnika. Posebna varnostna politika glede zahtevnosti, pogojev določanja, menjave, preteka ali drugih varnostnih parametrov s strani naročnika ni bila predana.

2.3.4.2 Prepoznavanje storitev

Prepoznavanje spletnih storitev poteka preko podatkov o digitalnem potrdilu za splošni namen, ki ga bo spletni servis – odjemalec uporabljal pri dostopu do spletnega servisa IS eZapori. Ti podatki vključujejo: ime izdajatelja (npr. SIGOV-CA), serijsko številko digitalnega potrdila (SN= 1234567891234) in njegovo veljavnost (npr. 11.11.2011-12.12.2012). Administrator IS eZapori podatke vpiše v varnostno shemo in dodeli dostopno vlogo.

2.4 Revizijska sledljivost

Standard ISO 27001 v svojem desetem poglavju Upravljanju s komunikacijami in produkcijo opredeljuje Spremljanje, katerega cilj je odkrivanje aktivnosti / dejavnosti nedovoljene obdelave ali dostopa do podatkov. V ta namen podaja smernice nadzora za beleženje revizijske sledljivosti, dnevnike za uporabnike z višjimi uporabniškimi pooblastili (Administrator in upravljavec) in

beleženje napak, ki jih v IS eZapori lahko zagotovi izvajalec. Ravno tako pomembna sklopa: nadzor sistemske porabe in sinhronizacija časa, pa ostajata v domeni naročnika (MJU-DEUP).

Informacijska in podatkovna varnost ter revizijska sledljivost predstavljajo enega glavnih in ključnih momentov v celotni življenjski dobi projekta. Razpoložljivost, sledljivost, nespremenljivost, varnost, integriteta in ne razkrivanje podatkov so ključni elementi rešitve eZapori.

Revizijska sled je zbirka vseh podatkov o vrednostih in njihovih spremembah ter povezanih dogodkih, ki so potrebni, da se predstavi verodostojni kronološki zapis in izluščijo informacije za ugotovitev in potrditev verodostojnosti. Omogoča, da se posamezni transakciji znotraj poslovnega dogodka retrogradno sledi do njenega nastanka. Nabor podatkov revizijske sledi morajo sestavljati vsi podatki, ki omogočajo identificirati potek transakcije in izluščiti informacije za določitev njene veljavnosti, pravilnosti in celovitosti. Hranjeni podatki morajo podpirati: verodostojnost, neoporečnost, nespremenljivost, razpoložljivost in nadzorovan dostop. Revizijska sled mora za zagotavljanje skladnosti z zakonodajo podpirati dve skupini ključnih dejavnikov. Prva je ugotavljanje zakonitosti, skladnosti in celovitosti obdelav, druga pa zagotavljanje verodostojnosti podatkov v primeru njihove uporabe v revizijskih in inšpekcijskih pregledih ter sodnih postopkih.

2.4.1 Revizijska sledljivost znotraj IS

Revizijska sledljivost znotraj IS eZapori bo zgrajena na dveh ravneh.

Prva raven zagotavlja aplikativno slednje spremembam pri ključnih poslovnih ali vsebinskih odločitvah. V ta namen bo za identificirane dele podatkovnega ali poslovnega modela vgrajeno zgodovinsko spremljanje sprememb zapisov z beleženjem podatkov v obsegu: kdo, kdaj, kaj, zakaj. Za polje »zakaj je bilo vpogledano v podatke« je potrebno pripraviti možnost vpisa razloga (npr: sodni nalog, odločba številka, ipd.). Pregledi zgodovine sprememb bodo del uporabniškega vmesnika (za točno določene, specifične in zelo pomembne vsebine), ki bo na voljo le za uporabnike s posebnimi pooblastili.

Nabor podatkov, ki zahtevajo revizijsko slednje znotraj IS, bo uporabnik (URSIKS) podrobneje določil znotraj funkcionalnih specifikacij [3] ob podrobnejši analizi vsebine.

2.4.2 Oracle Audit Vault

Druga raven je namenjena zagotavljanju revizijske sledi za podatkovne poizvedbe in opravila (jobi, obdelave,…) in dostope do podatkov iz sistemskega (upravljanje, administracija) stališča. Za beleženje, dostopanje in varno pregledovanje zapisov revizijske sledi za podatkovne obdelave, ki jih bo naročnik določil kot revizijsko sledljive, bo v okviru druge ravni nadzora poskrbljeno z licenčno programsko rešitvijo Oracle Audit Vault, ki jo kot del infrastrukture, kjer bo gostovala rešitev eZapori zagotavlja MJU-DEUP. Ker je celotna infrastruktura v upravljanju in vzdrževanju MJU mora naročnik z MJU dogovoriti pravila uporabe, dostopa, vpogleda in upravljanja z revizijskimi sledmi znotraj Audit Vault.

Oracle AV dejansko zagotavlja zbiranje ter analiziranje revizijskih zapisov dostopov do podatkov v podatkovnih zbirkah. Z njim se je konsolidiralo revizijske silose prek celotnega sistema in varno shranilo revizijske podatke na eni lokaciji.

Sledenje aktivnosti na transakcijski in arhivski bazi je realizirano z Oracle Audit Vault (AV) agentom. AV agent zbrane revizijske podatke pošlje na AV strežnik, kjer jih je možno pregledati, analizirati, izdelati poročila in opozorila z namenskim AV orodjem. Samodejna (programska) obdelava podatkov bo ločena z uporabo zasebnega uporabnika na bazi. Tudi zunanje aplikacije, ki se povezujejo na eZapori kot odjemalci, bodo imele ločena uporabniška imena, kar pomeni, da bo vsak odjemalec zaseben uporabnik na bazi. Ugotavljanje osebe, ki je sprožila zahtevek bo narejeno na podlagi imena odjemalca, številke transakcije in podatkov o uporabniku, ki je sprožil transakcijo iz aplikacije odjemalca.

Dodatno je povsem onemogočen dostop do revizijskih sledi za administratorje. Administratorjem ni dana možnost naknadnega popravljanja, spreminjanja ali brisanja delov ali celotnih revizijskih sledi. Znotraj sistema Oracle AV nihče nima nenadzorovane možnosti popravljanja revizijskih sledi, ki se nanašajo na njegove ali aktivnosti drugih, prav tako ni nikomur omogočen neopazen »izklop« beleženja revizijskih sledi.

Nabor podatkov, ki zahtevajo revizijsko slednje bo podrobneje določen znotraj funkcionalnih specifikacij [3] ob podrobnejši analizi vsebine.

2.5 Podatkovni model

Vsi podatki aplikacije eZapori bodo shranjeni v shemi EZAPORI_DATA. Slednja shema bo zaklenjena in nihče se ne bo neposredno nanjo prijavljal. Vse evidence bodo dostopne preko baznih API procedur in baznih vpogledov. Principelno se hranijo podatki evidenc ločeno po logičnih vsebinskih področjih in ločeno glede na podatke in metapodatke (indeksi) po »tablespaceih«.

Aplikacija nikoli direktno ne dostopa do podatkov v shemi EZAPORI_DATA temveč preko »proxy« shem, ki imajo dodeljen minimalen nabor pravic in baznih APIjev. Nabor shem bo znan po podrobni analizi glede na varnostne zahteve in funkcionalno dekompozicijo aplikacije.

Podatkovni model bo izdelan po izvedbi podrobne analize posamezne funkcionalne celote. Ob izdelavi se bo sledilo principom uporabnosti skupnih šifrantov med ločenimi funkcionalnimi celotami, normaliziranosti fizičnega modela podatkov in v največji možni meri uporabi že obstoječega modela aplikacije iEZO.

2.6 Integracija z zunanjimi podatkovnimi zbirkami

Predvideni spletni servisi in smer pretoka informacij so prestavljeni v dokumentu Analiza_procesi_v1.0
Vsebina in delovanje bo podrobneje določen znotraj funkcionalnih specifikacij [3] ob podrobnejši analizi vsebine.

2.7 Infrastrukturna izhodišča

Infrastrukturna izhodišča za referenčno, testno, uvajalno in produkcijsko okolje predpisuje naročnik oziroma: MJU-DEUP in Ministrstvo za pravosodje, kot ponudnika infrastrukture. Osredji del izhodišč povzemajo navedeni referenčni dokumenti: [1] - [7].

Okolij, znotraj katerih bo grajeno, testirano, preverjano in kjer bo potekalo izobraževanje in produkcija je več. V splošnem ločimo:

- okolje izvajalca (samostojno razvojno in testno okolje, skladno s produkcijsko infrastrukturo naročnika);
- okolje naročnika (gostovanje pri MJU) sestavljajo referenčno, testno in izobraževalno ter produkcijsko okolje,
- okolje naročnika (gostovanje pri MP) sestavljajo testno (QA) in produkcijsko okolje.

2.7.1 Odlagališče izvorne kode

Zahteva naročnika je, da se vsa izvorna koda, pripravljena s strani izvajalca, odlaga v odlagališče izvorne kode pri MJU (sistem SVN). V ta namen je na voljo spletna storitev na naslovu »**eZapori-svn.pdcext.sigov.si:443/eZapori/**«, dosegljiva preko varovanega, namenskega dostopa. Za posredovanje in odlaganje izvorne kode pripravljene s strani naročnika navedenega vira je zadolžen uporabnik (URSIKS).

MJU je znotraj referenčnega dokumenta **Drevesna struktura odlagališča kode SVN na MJU, [3]** podal zahtevano strukturo znotraj SVN odlagališča izvorne kode.

Ministrstvo za pravosodje posebnih zahtev glede odlaganja izvorne kode ni predalo, zato bo vsa izvorna koda predana skladno s pogodbenimi določili.

Pravila za uporabo repozitorija kode (SVN) pri MJU-DEUP:

- Koda se mora v SVN sistem naročnika odlagati v vse smiselne vrste datotek razen binarnih datotek (izloči bin, obj, Debug, Release in podobne mape, binarne datoteke, izhode avtomatskih testov…)
- Vsak, ki prenaša kodose prijavi z svojim uporabniškim imenom.
- Vsi bodo imeli dostop za branje (update). Za pisanje (commit) se dostop razdeli po mapah in ustreznih analitikih ter razvijalcih.
- Obvezno je redno posodabljanje (commit) v glavno vejo.
- Obvezna je uporaba smiselnih commit sporočil.

SVN struktura vsebuje tudi imenike za področje objektov podatkovne zbirke:

- dokumentacijo podatkovne zbirke,
- specifikacijo logičnega modela,
- navodila za izdelavo fizičnega modela,
- navodila za namestitev fizičnega modela,
- izvorno kodo baznih objektov (DDL stavke),
- skripte za namestitev/odstranitev objektov podatkovne zbirke,
- skripte za polnjenje tabel s podatki,
- skripte za nadgradnjo objektov podatkovne zbirke,
- skripte za testiranje podatkovne zbirke.

MJU-SVN drevesna struktura v0.6							
SVN-root	*I. Nivo*	*II. Nivo*	*III. Nivo*	*IV. Nivo*	*V. Nivo*	*VI. Nivo*	*Opis*
<NazivNaročnika/ProgramProjektov>							Korenski direktorij za posamezne državne organe ali programe projektov
	<Projekt>						korenski imenik posameznih projektov, v primeru programa projektov pa podprojekt
		<Aplikacija>					ena od aplikacij/skopov za danega naročnika, na tem nivoju se dodeljujejo pooblastila zunanjim izvajalcem, ta nivo ustreza tudi enoti namestitve (deployu)
			<db_poizvedbe>				
				<log>			logi izvajanja skript
				<sql>			AD-HOC SQL skripte
			<trunk>				
				<dokumentacija>			
					<OVSP>		Dokumenti po OVSP in RTP postopku
					<uporabniska>		Navodila za uporabo
					<tehnicna>		Tehnična dokumentacija projekta
					<namestitvena>		Namestitvena navodila za bazni in aplikativni del skupaj.
					<testna>		Testni vzorci, testni scenariji in poročila o testiranju (regresijskem, obremenitvenem, generalnem preizkusu). Tukaj je tudi tabela TAG-iranih namestitev na TEST/SOLA/PROD okolje
				<app_objekti>			
					<build>		Build skripta s pripadajočo nastavitveno datoteko v kateri so vsi parametri, ki se spreminjajo glede na okolje (TEST/SOLA/PROD).
					<config>		Konfiguracijske datoteke, ki jih potrebuje aplikacija, s pripadajočimi nastavitvenimi datotekami v katerih so vsi parametri, ki jih potrebuje aplikacija.
					<deploy>		Namestitvene datoteke (.ear, .war ...). Ime datoteke mora biti v obliki npr. "Projekt_Aplikacija_Sklop.ear"
					<resources>		Razni viri potrebni za delovanje aplikacije
						<lib>	Knjižnice, ki bi jih aplikacija potrebovala za svoje delovanje in se ne dajo vključiti v EAR.
					<src>		
						<sklop 1>	
						<sklop 2>	
						...	
					<kriticni_popravki>		Za izjemne primere, ko je produkcija po tleh ...
						<"datum"_"ura">	
				<bazni_objekti>			
					<dba>		V ta imenik se odlagajo poročila/rezultati/logi namestitev
						<info>	druge informacije o posebnostih MJU okolja
						<log>	Namenjen odlaganju log datotek, ki nastanejo v postopku nameščanja sql skript iz direktorijev deploy in kriticni_popravki.
					<src>		Vsebuje kodo za polno namestitev baznih objektov določene verzije.
					<deploy>		Sql skripte, s katerimi se nadgradi verzija baze N na verzijo baze N+1
					<kriticni_popravki>		Sql skripte za odpravo točno določenega problema, ki se je pojavil na produkciji.
						<"datum"_"ura">	
			<tags>				
				<verzija 1>			Dejanska verzija aplikacije npr. 1.2.39, vendar je zaradi preglednosti nujna uporaba vodilnih ničel. Tako dobimo imenik "001.002.039".

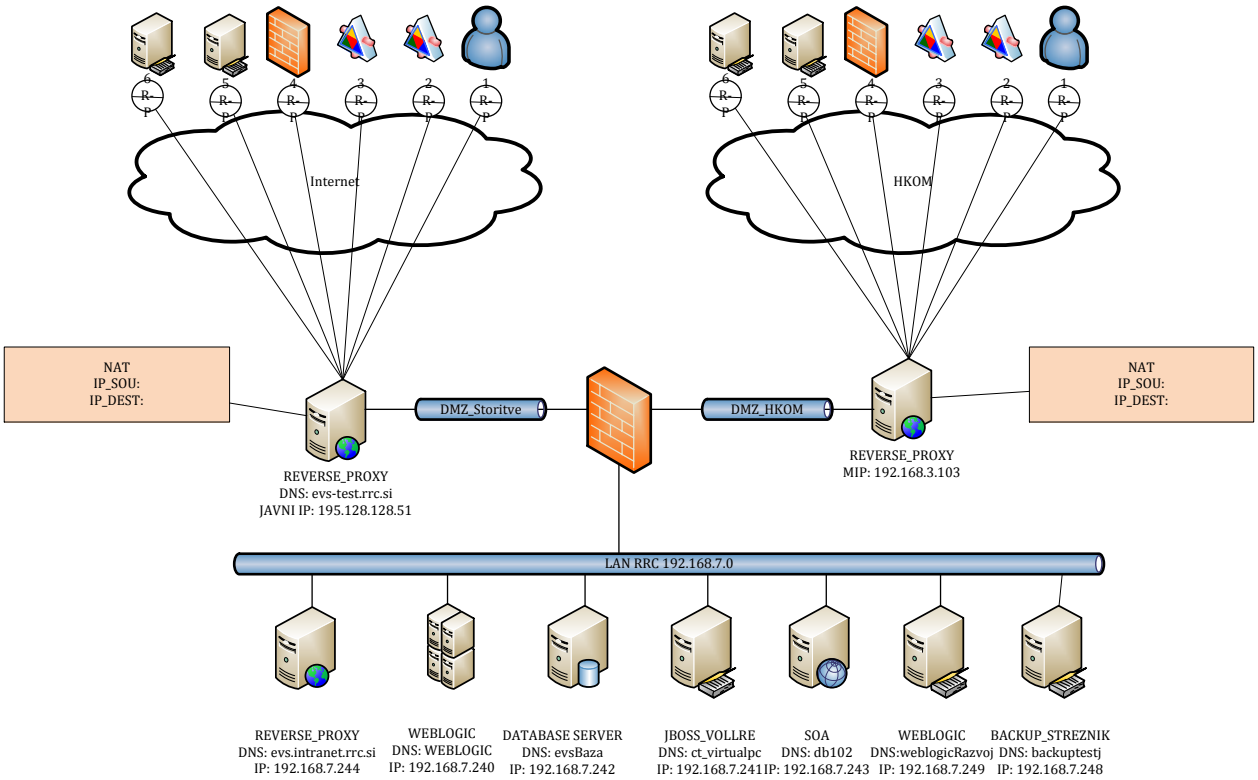
V primerjavi s predpisano MJU strukturo sta na stran izvajalca dodani dve mapi za kodo in sicer:

- WS - za spletne servise,
- GUI - za uporabniški vmesnik.

2.8 Razvojno okolje

Razvojno okolje zagotavlja izvajalec. Stopnja integracije s sistemi naročnika je le preko repozitorija/skladišča kode. Gradniki razvojnega okolja izvajalca zagotavljajo:

- Razvojna orodja,
- Repozitorij/skladišče kode z integracijo z repozitorijem kode naročnika,
- Repozitorij/skladišče dokumentov in forum za izmenjavo informacij,
- Programsko okolje projektne pisarne (s podporo spremljanja sprememb, reklamacij in razhroščevanja kode),
- Neprekinjeno integracijo.



Slika 6; Razvojno okolje IS eZapori - RRC

Raven	Gradnik	DNS ime
Raven dostopa do podatkov	Database: Oracle Database 11g EE Release: 11.2.0.2.0 – 64 bit	
Raven izmenjave podatkov	JBoss 5.1 JAX-WS (2.2) support JBoss Application Server 5 (JavaEE 5 compliant)	
Poslovna raven	Application Server: Oracle WebLogic 11g R1, release: 10.3.3	
Podporne storitve	– Odlagališče kode – Projektna pisarna – Odlagališče dokumentov	tfs.intranet.rrc.si oaza.intranet.rrc.si portal.intranet.rrc.si

Gradnike razvojnega okolja sestavljajo:

- Razvojna orodja (Oracle, Forms, Java, WS)
- Podporne storitve (projektna pisarna, odlagališče izvorne kode, podpora dokumentaciji projekta,…)

2.8.1 Razvojna orodja

V procesu razvoja IS eZapori bodo uporabljena naslednja razvojna orodja

- Oracle in razvojno okolje spletnih storitev sestavljajo:
- Oracle Designer.
- NetBeans,
- Quest: Code tester for Oracle
- Oracle Forms, Oracle Reports,
- Oracle Discoverer
- Oracle Application Express.

- Java razvojno okolje sestavljajo naslednji gradniki:
- Oracle Java SE 6 JDK
- JBoss AS Community Edition 5.1
- Maven (orodje za gradnjo in upravljanje projektov)
- Eclipse IDE for Java EE Developers Helios SR2 + z dodatki (plug-in):
    - M2Eclipse - Maven plugin (http://m2eclipse.sonatype.org)
    - Subclipse - Subversion plugin (http://subclipse.tigris.org).

2.8.2 Odlagališče dokumentov in forum

Izvajalec za odlagališče dokumentov in forum izvajalcev uporablja Share Point portal, kjer ima projekt eZapori dodeljeno lokacijo z urejenimi pravicami dostopa. Dostop zunanjih uporabnikov je urejen preko VPN povezav z osebno avtentikacijo.

2.8.3 Projektna pisarna, nadzor sprememb in napak

Za potrebe projektne pisarne, ki izvaja spremljanja projekta, nadzor nad spremembami in upravljanje z reklamacijami, bo izvajalec uporabljal lastno spletno rešitev Oaza.

2.9 Referenčno Javansko izvajalno okolje MJU

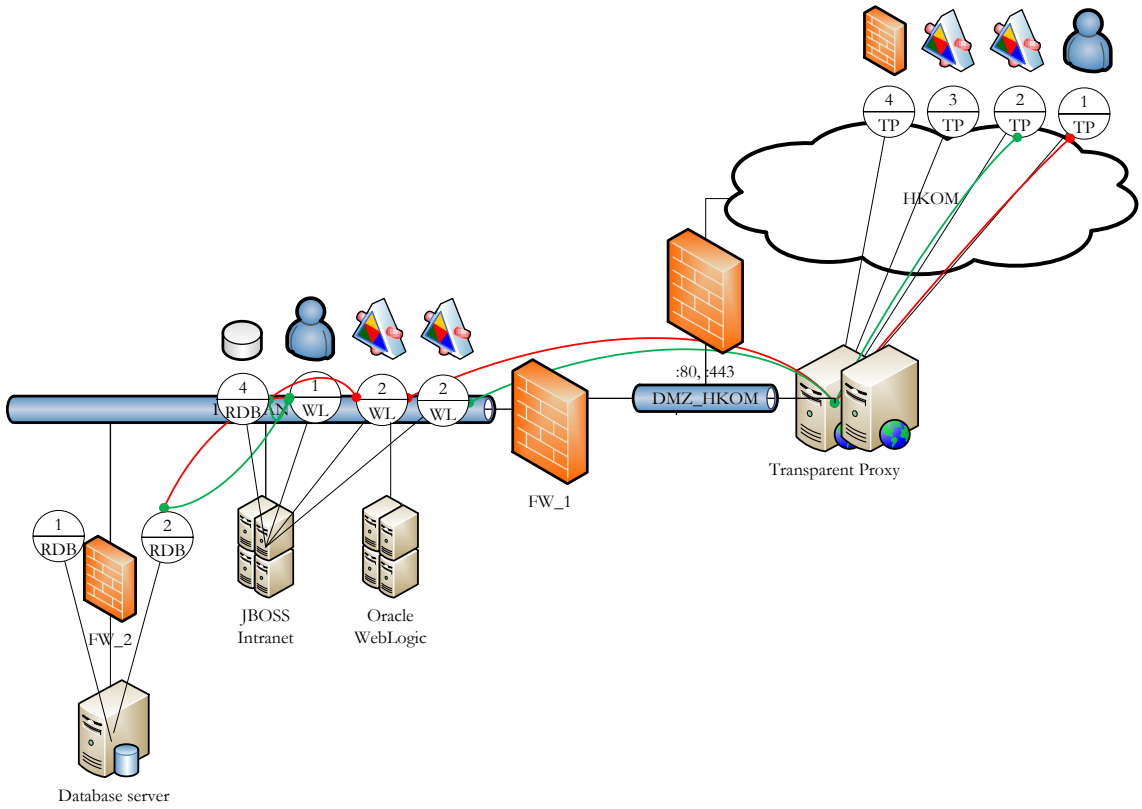
Referenčno izvajalno okolje je namenjeno preverjanju delovanja IS eZapori pred predajo v testno okolje MJU. Predstavlja osnovo preverjanja odprtosti delovanja spletnih storitev, neodvisno od testnega in produkcijskega okolja naročnikove infrastrukture. Okolje je namenjeno testiranju uspešnosti namestitve in izvedbe funkcionalnih testov in predstavlja prvo kontrolno točko v procesu implementacije IS eZapori na ciljno infrastrukturo. Referenčno javansko izvajalno okolje JEE temelji na odprtokodnem javanskem aplikacijskem strežniku JBOSS verzije 5.1. Povzetek referenčnega okolja je povzet v spodnji preglednici, podrobnejše specifikacije pa so opredeljene v dokumentu [4]

Referenčno Javansko izvajalno okolje		
Opcijska oprema	**programska**	PostgresPlus Advanced Server 8.4, JBoss Enterprise Application Platform 5, JBoss Enterprise SOA Platform 5.
Dodatna oprema	**programska**	Java 6 Runtime Environment, JBoss Community Edition 5.1, JBoss ESB 4.9, Gonilniki JDBC,

	PostgreSQL 8.4, PostgresPlus 8.3 R2, DB2 UDB 9.5, Oracle 11g.
Aplikativna programska oprema	Apache 2.2, PostgreSQL 8.4,
Operacijski sistemi	Red Hat Enterprise Linux 5.5 (x86_64)
Virtualizacija	VMWare, Oracle VM

Referenčno izvajalno okolje VOLRRE je izvajalec prevzel na MJU-DEUP in predstavlja osnovo njegovega referenčnega okolja.

Znotraj krovne analize procesov so opredeljeni procesi podatkovne integracije, smer njihove povezave in zunanji informacijski sistemi ali podatkovne zbirke s katerimi se dopolnjujejo.



Slika 7; Referenčno in testno okolje JEE pri MJU

2.10 Testno okolje

2.10.1 Testno okolje izvajalca

Testno okolje izvajalca bo nameščeno v sklopu centralne strežniške infrastrukture RRC in mora biti v vseh pogledih enakovredno produkcijskemu okolju. Sestavljata ga dva ključna segmenta in sicer **razvojni testni segment** in **obremenilni testni segment** namenjen varnostnim, performančnim in obremenilnim testiranjem.

Testni segment izvajalca (razvojni in obremenilni) je namenjen:

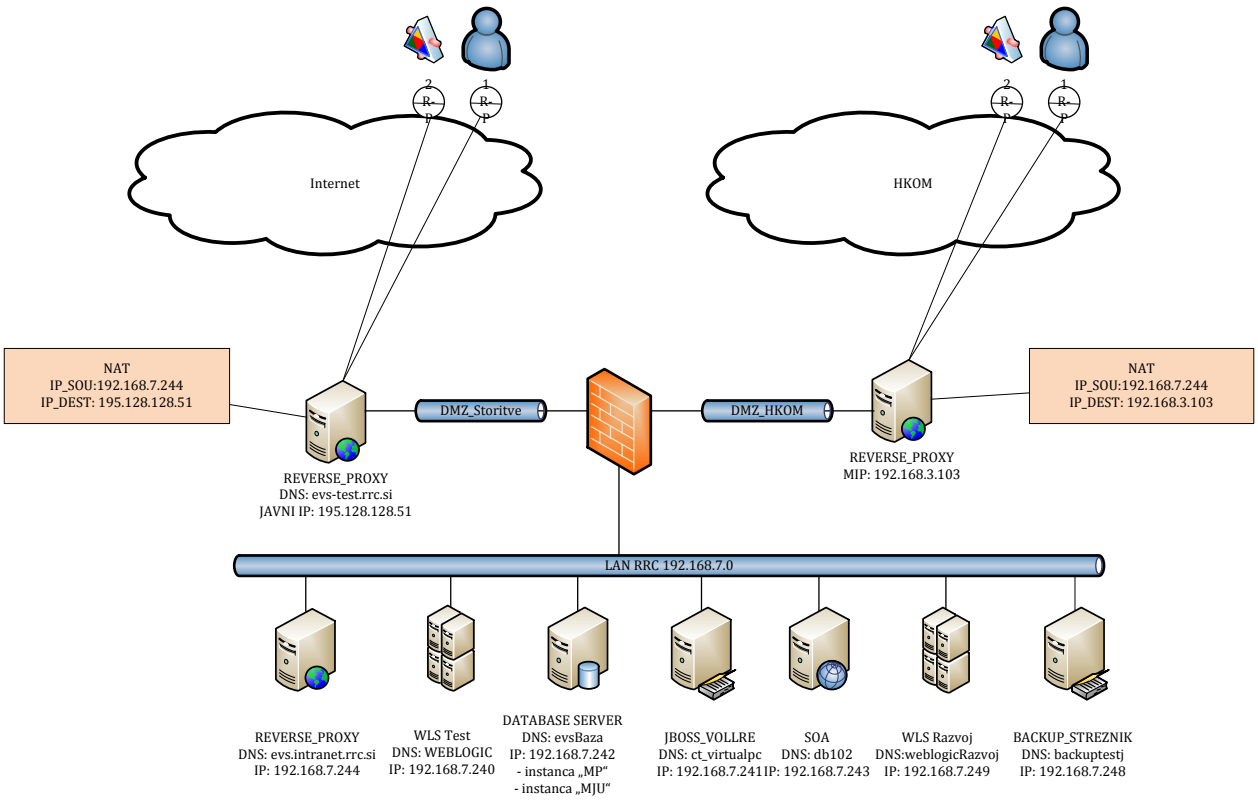
- potrditvenemu testiranju,
- integracijskemu testiranju,
- avtomatiziranemu testiranju uporabniškega vmesnika in podatkovnih integracij,

- obremenilnemu testiranju (večje število odjemalcev, večji število podatkovnih integracij,…)
- testiranju v pogojih poslabšanja lastnosti ključnih transportnih poti (QoS),
- testiranju v pogojih strogega omejevanje prometa s stališča varnostni (prepustnost TCP/IP naslovov in vrat),
- varnostnemu testiranje razpoložljivih gradnikov in storitev.

Obremenilni testni segment vklopimo na uporabniški in komunikacijski strani z mehanizmi kot so:

- na komunikacijski opremi s funkcionalnostjo QoS za simulacijo zmanjševanja pasovne širine transportnih poti,
- na požarni pregradi z omejevanjem prepustnosti TCP/IP prometa (naslovi in vrata/ports),
- na strani odjemalcev in podatkovnih integracij s simulacijo večjih obremenitev vnosa, branja in obdelave,
- na strani strežnikov s poslabšanjem lastnosti (spomin, procesor) strojne opreme.

V sklopu testnega okolja delujejo vse storitve pod enakimi funkcionalnimi (in ne njuno tudi performančnimi pogoji) kot delujejo v produkcijskem okolju.



Slika 8; Referenčno in testno okolje izvajalca, razvojno, integracijsko in obremenilno testiranje

Raven	Gradnik	DNS ime
Strežnik gostitelj	Oracle VM Server	IP: 192.168.7.254
	Oracle VM Manager: - Oracle Linux 5.3 64bit - Oracle VM Manager	IP: 192.168.7.253 Dostop do VM Manager: http://192.168.7.253:8888/OVS

Raven dostopa do podatkov	OTN developer days-baza: – Oracle Linux 5, – Oracle Database 11*g* Release 2 Enterprise Edition, – Oracle TimesTen In-Memory Database Cache, – Oracle XML DB, – Oracle SQL Developer, – Oracle SQL Developer Data Modeler, – Oracle Application Express 4.0, – Oracle JDeveloper, – Hands-On-Labs (accessed via the Toolbar Menu in Firefox)	IP: 192.168.7.242 Dostop do Oracle EM: https://192.168.7.242:1158/em
Raven izmenjave podatkov	SOA referenčno okolje: JBoss 5.1 JAX-WS (2.2) support JBoss Application Server 5 (JavaEE 5 compliant) web service stack EJB 2.1, EJB3 and JSE endpoints Attachments Profile Version 1.0 Support for MTOM/XOP and SwA-Ref WS-Security 1.0 for XML Encryption/Signature of the SOAP message WS-Addressing (W3C candidate release) and JSR-261 WS-ReliableMessaging WS-Eventing WS-Policy	IP: 192.168.7.243
Referenčno okolje	JBoss referenčno okolje – Volrre model	IP: 192.168.7.241
Poslovna in predstavitvena raven	Oracle WebLogic: – Oracle linux 5.6 64 bit – WebLogic	IP: 192.168.7.240 Dostop do Weblogic: http://192.168.7.240:7001/console

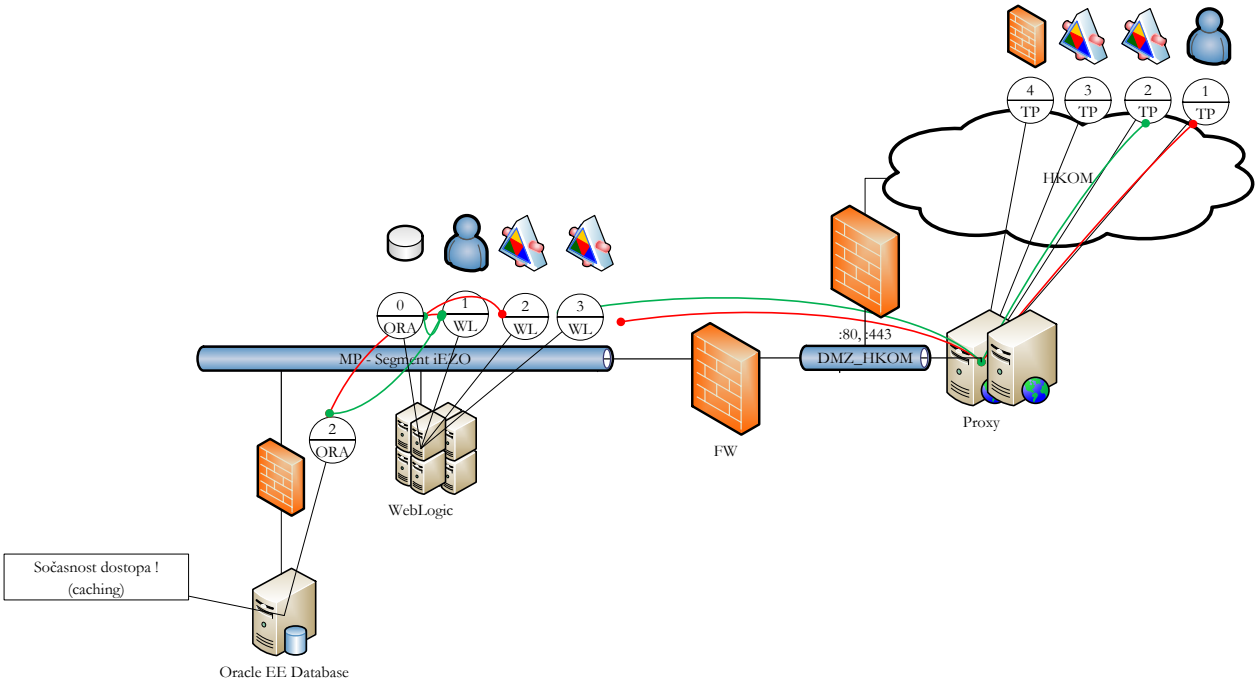
Vsa gesla za dostop do okolja so hranjena v repozitoriju gesel RRC, KeePass PasswordSafe.

2.10.2 Testno okolje naročnika

Testno okolje naročnika sestavljata dve infrastrukturni okolji:

- okolje, nameščeno v sklopu centralne strežniške infrastrukture Ministrstva za javno upravo in
- okolje, nameščeno v sklopu centralne strežniške infrastrukture Ministrstva za pravosodje.

Testno okolje mora biti v vseh pogledih enakovredno produkcijskemu okolju. Namenjeno je potrditvenemu testiranju (torej preverjanju, ali je bil nek popravek/nadgradnja/razvoj izveden v skladu z željami naročnika; testiranje pravilnosti kode se izvaja na strani izvajalca) s strani naročnika. V sklopu testnega okolja delujejo vse storitve pod enakimi funkcionalnimi (in ne njuno tudi performančnimi) pogoji kot delujejo v produkcijskem okolju.



Slika 9; Testno okolje naročnika, MP

Testno, izobraževalno in okolje za zagotavljanje kakovosti - MP	
Reverse-Proxy	Apache: httpd-2.2.3-45.el5.centos.1 CentOS v5.4, Oracle VM
Spletni strežnik	Apache: httpd-2.2.3-45.el5.centos.1 CentOS v5.4, Oracle VM
Load balancer	Apache httpd-2.2.3-45.el5.centos.1 CentOS v5.4, Oracle VM
Aplikativni strežnik	Apex Listener: 1.1.3 Oracle WebLogic 11gR1 (10.3.2), Java JRockit (jdk1.6.0_20-R28.1.0-4.0.1)
Relacijska baza	Oracle Enterprise Edition 11.2.0.1 – 64 bit

2.11 Produkcijsko okolje

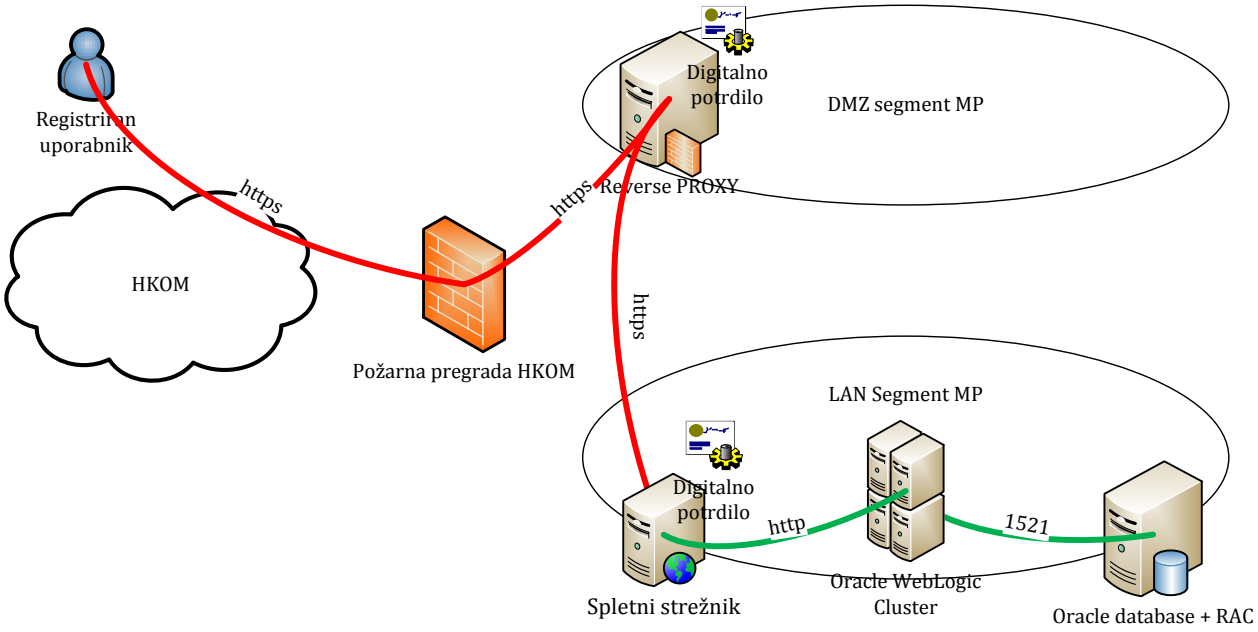
Osnovni del IS eZapori bo nameščen v sklopu centralne strežniške infrastrukture Ministrstva za javno upravo. Namenjeno je produkcijskemu delovanju glavnih modulov IS eZapori in vseh njegovih storitev v notranjem - intranetnem segmentu HKOM, kot tudi podatkovnim integracijam. Za delovanje IS eZapori znotraj produkcijskega okolja veljajo pravila, kot jih določa lastnik in vzdrževalec infrastrukture MJU DEUP.

Drugi del produkcijskega okolja IS eZapori predstavlja infrastruktura, nameščena v sklopu centralne strežniške infrastrukture Ministrstva za pravosodje. Namenjeno je produkcijskemu delovanju izbranih modulov IS eZapori in njihovi podatkovni integraciji s središčnim in zalednimi IS naročnika in Ministrstva za pravosodje. Za delovanje IS eZapori znotraj produkcijskega okolja veljajo pravila, kot jih določa lastnik in vzdrževalec infrastrukture MP.

2.11.1 Produkcijsko okolje MP (APEX)

Osnovne gradnike testne in izvajalne infrastrukture okolja APEX na MP predstavljajo:

- **Požarna pregrada**; med omrežjem HKOM in DMZ segmentov MP; upravlja, nadzira in prepušča promet (port 80, 443) med omrežnimi segmenti,
- **Reverse Proxy strežnik**; zaključuje zunanji http/https promet, hrani javna digitalna potrdila za razpoznavanje in medsistemsko povezovanje,
- **Spletni strežnik**;
- **Visoko razpoložljivi Oracle WebLogic aplikacijski strežnik**; skrbi za aplikacijsko strego, gosti vmesno APEX in drugo aplikacijsko infrastrukturo, deli in usmerja promet,
- **Visoko razpoložljiva Oracle podatkovna baza.**



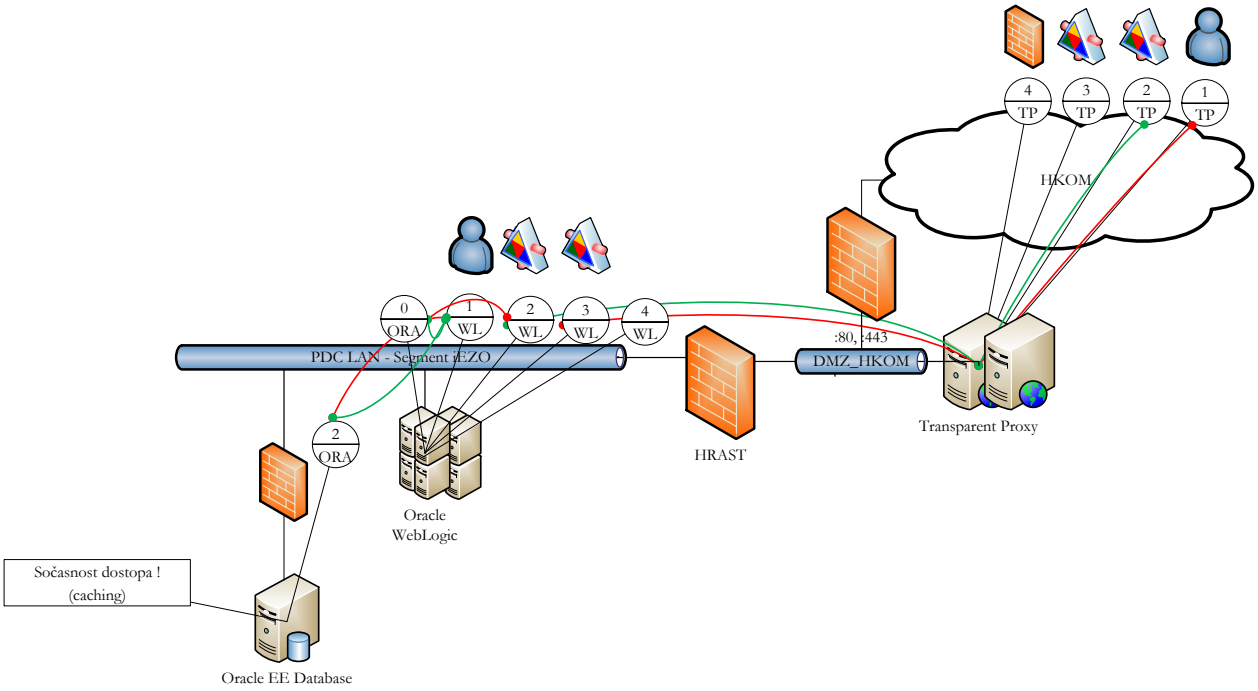
Slika 10: Infrastruktura Ministrstva za pravosodje

Produkcijsko okolje - MP	
Reverse-Proxy	Apache: httpd-2.2.3-45.el5.centos.1 CentOS v5.4, Oracle VM
Spletni strežnik	Apache: httpd-2.2.3-45.el5.centos.1 CentOS v5.4, Oracle VM
Load balancer	Apache httpd-2.2.3-45.el5.centos.1 CentOS v5.4, Oracle VM
Aplikativni strežnik	Apex Listener: 1.1.3 Oracle WebLogic 11gR1 (10.3.2), Java JRockit (jdk1.6.0_20-R28.1.0-4.0.1)
Relacijska baza	Oracle Enterprise Edition 11.2.0.1 – 64 bit

Produkcijsko okolje naročnika bo nameščeno tudi v sklopu centralne strežniške infrastrukture Ministrstva za javno upravo. Namenjeno je produkcijskemu delovanju IS eZapori in vseh njegovih storitev v notranjem (intranetnem segmentu HKOM) omrežju. Za delovanje IS eZapori znotraj produkcijskega okolja veljajo pravila, kot jih določa lastnik in vzdrževalec infrastrukture MJU-DEUP. Osnovne gradnike testne in izvajalne infrastrukture okolja MJU.DEUP predstavljajo:

- **Sistem požarnih pregrad**; med segmenti in omrežji z različnimi varnostnimi stopnjami in pooblastili ; upravlja, nadzira in prepušča promet med omrežnimi segmenti,
- **Posredniški strežniki (Transparent, Reverse Proxy strežniki)**; posredujejo in zaključujejo zunanji (intranet HKOM) in notranji (lokalni) http/https promet, hranijo javna digitalna potrdila za razpoznavanje in medsistemsko povezovanje,
- **Spletni strežniki**; hranijo in posredujejo statične spletne vsebine,
- **Visoko razpoložljivi Oracle WebLogic aplikacijski strežnik**; skrbi za aplikacijsko strego, gosti vmesno APEX in drugo aplikacijsko infrastrukturo, deli in usmerja promet,
- **Visoko razpoložljiva Oracle podatkovna baza,**
- **Orodja (Audit Vault, Oracle Discoverer, ipd);** zagotavljajo podporne storitve IS eZapori.

Produkcijsko okolje MJU-DEUP		
Raven	Gradnik	DNS ime
Raven dostopa do podatkov	Database: Oracle Database 11g EE Release: 11.2.0.2.0 – 64 bit (podrobnosti: glej RTP okolje raven dostopa do podatkov)	
Raven izmenjave podatkov	Java 6 Runtime Environment, JBoss Community Edition 5.1, JBoss ESB 4.9, Gonilniki JDBC, PostgreSQL 8.4, PostgresPlus 8.3 R2, DB2 UDB 9.5, Oracle 11g.	
Poslovna in predstavitvena raven	Application Server: Oracle WebLogic 11gR1 (10.3.3) Oracle FORMS 11g, Java JRockit (jdk1.6.0_20-R28.1.0-4.0.1) SUSE Linux, 64 bit ali OEL v5, 64 bit VMWare ali Oracle VM	



Slika 11: Produkcijsko okolje MJU-DEUP

3 Upravljanje z informacijskimi tveganji

3.1 Informacijska tveganja in uporabljeni nadzor

Pri pripravi rešitve za projekt eZapori, so bila upoštevana ključna informacijska varnostna tveganja in smernice oziroma vodila za njihovo odpravo. Omenjena varnostna tveganja so vsebinsko razdeljena v dva sklopa in sicer:

- **Regulativna varnostna tveganja**; Sklop s stališča veljavne zakonodaje, priporočil Informacijskega pooblaščenca (pogled varstva osebnih podatkov) in standardov (predvsem ISO 27001 in ISO 27002) identificira in opredeljuje tveganja in podaja pristope za njihovo zmanjšanje.
- **Infrastrukturna varnostna tveganja**; Sklop s tehnološkega stališča ugotavlja in opredeljuje tveganja IS eZapori in podaja pristope in uporabljene tehnologije za njihovo odpravo, ki jih lahko implementira izvajalec.

Za zmanjševanje ključnih informacijskih varnostnih tveganj so bili prepoznani in upoštevani ustrezni informacijski varnostni nadzorni mehanizmi, ki temeljijo na referenčnih dokumentih ter načelih dobre prakse pri razvoju informacijskih sistemov.

Ključna informacijska varnostna tveganja ter prepoznane in upoštevane varnostne kontrole so navedeni v nadaljevanju tega poglavja.

3.1.1 Regulativna varnostna tveganja

Standard ISO 27001 v poglavju Skladnost, podaja smernice in kontrolne točka za zagotavljanje skladnosti informacijskih rešitev z zakonskimi zahtevami. V ta namen je potrebno določiti:

- **Skladnost z zakonskimi zahtevami**; kar pomeni: določitev veljavne zakonodaje, pravice intelektualne lastnine, zaščita organizacijskih/projektnih zapisov, varstvo podatkov in zasebnost osebnih podatkov, preprečevanje zlorabe objektov za obdelavo podatkov, spoštovanje uredb o kriptografskem nadzoru.
- **Skladnost z varnostnimi politikami in standardi** in preverjanje tehnične skladnosti
- **Nadzor informacijskih sistemov**; kar obsega pregled nadzora informacijskega sistema in pregled sistema zaščite informacijskih orodij.

3.1.1.1 Zaupnost

Zaupnost znotraj informacijskega sistema zagotavlja varovanje osebnih podatkov ter informacij pred razkritjem nepooblaščenim osebam in zagotavljanje odgovornosti za dejanja pooblaščenih oseb. V veliki meri mehanizme nadzora zaupnosti rešujejo interni organizacijski predpisi naročnika, mehanizmi revizijskega sledenja in arhitekturna zasnova IS. Zaupnost je integrirana v vse dele IS, njene zahteve so obravnavane znotraj vseh podrobnejših členitev.

3.1.1.2 Celovitost

Celovitost, ki pomeni:

- varovanje podatkov in informacij pred nepooblaščenimi spremembami na celotni podatkovni poti od izvora (vnos, podatkovna integracijska točka) do ponora (podatkovna hramba),
- zagotavljanje dokazljivosti izvora in verodostojnosti,
- neokrnjenosti in nespremenljivosti informacij in postopkov procesiranja,

je vgrajena v IS eZapori od načrta do izvedbe oziroma delovanja, njene zahteve so obravnavane znotraj vseh podrobnejših vsebin.

Podatkovna celovitost IS eZapori omogoča določitev zahtev podatkovne kakovosti. Podatki, ki dostopa jo do podatkovne hrambe (relacijske baze Oracle) morajo te zahteve izpolniti. Če uporabnik/sistem/podatkovna integracija poskuša vstaviti podatek, ki ne izpolnjuje takšne zahteve, bo podatek zavrnjen, podatkovni vir pa obveščen o kršitvi podatkovne celovitosti. Tipične uporabljene omejitve podatkovne celovitosti so: Not Null, Unique Key, Primary Key, Foreign Key, Check.

3.1.1.3 Razpoložljivost

Razpoložljivost pomeni zagotavljanje dostopa pooblaščenim osebam do informacij in pripadajočih sredstev, ko jih potrebujejo.

Naročnik je v razpisni dokumentaciji določil razpoložljivost IS eZapori:

- znotraj delovnega časa naročnika; za lastno uporabo,
- 24 ur vse dni v letu; za zunanje uporabnike in informacijske sisteme povezanih institucij eZapori.

Redne posodobitve in tehnične izboljšave eZapori bodo v sodelovanju z naročnikovim sistemskim inženiringom izvedene tako, da to ne bo pomenilo nedelovanja eZapori. V ta namen bodo pri izvajalcu vzpostavljena: razvojno, referenčno in testno okolje. Glede na porazdeljenost IS eZapori med infrastrukturo MJU in MP so predvidena naslednja okolja:

- MJU: referenčno, testno/izobraževalno in produkcijsko okolje
- MP: testno/QA okolje in produkcijsko okolje.

Cilj vseh okolij pri naročniku in izvajalcu je zagotoviti optimalne pogoje za delovanje IS eZapori.

V kolikor se nedelovanju eZapori ni mogoče izogniti, naročnik predvideva tehnološke (orodja za neprekinjeno integracijo, sledenje spremembam,…) in poslovne (postopki, navodila) mehanizme, ki pomagajo obvladovati tveganja. Zahteva naročnika je, da mora biti vsaka načrtovana prekinitev delovanja (zaradi npr. nujnih popravkov programske ali strojne opreme, nadgradenj in drugih nujnih del) naročniku sporočena najmanj 3 dni pred dejansko prekinitvijo. V sporočilu mora biti naveden razlog za prekinitev ter čas v katerem bo izvedena prekinitev. Načrtovana prekinitev delovanja eZapori se lahko izvede v nočnem času od 23h zvečer do 4h zjutraj.

3.1.1.4 Zakonska skladnost

Rešitev eZapori mora biti skladna z veljavno zakonodajo v Republiki Sloveniji. Področne Zakonske osnove so podrobneje opredeljene v analizi projekta in so:

- Kazenski zakonik,
- Zakon o kazenskem postopku,
- Zakon o zaščiti prič,
- Zakon o prekrških,
- Zakon o izvrševanju kazenskih sankcij,
- Zakon o sodelovanje v kazenskih zadevah z državami članicami EU,
- Zakon o varstvu osebnih podatkov,
- Zakon o upravnem postopku,
- Zakon o elektronskem poslovanju in elektronskem podpisu,
- Zakon o upravnih taksah,
- Pravilnik o izvrševanju kazni zapora,
- Pravilnik o izvrševanju pripora,
- Pravilnik o izvrševanju vzgojnega ukrepa oddaje mladoletnika v prevzgojni dom,
- Pravilnik o načinu zbiranja podatkov in vodenju zbirke podatkov o obsojencih,
- Pravilnika o izvrševanju pooblastil in nalog pravosodnih policistov,
- Interno navodilo o vodenju in zavarovanju osebnih podatkov v UIKS.
- Navodilo o dostopu do aplikacije eZapori.

S stališča informacijske varnosti in upravljanja z informacijskimi tveganji pa so pomembni še:

- Zakon o varstvu osebnih podatkov,
- Zakon o varovanju tajnih podatkov,
- Zakon o elektronskem poslovanju in elektronskem podpisu.

3.1.1.5 Skladnost s standardi in priporočili

Zahteva naročnika je, da mora biti rešitev eZapori skladna s standardom ISO 27001 in 27002 v poglavjih, ki se nanašajo/navezujejo na informacijsko varnost in revizijsko sledljivost. Informacijska sistem eZapori bo od faze načrtovanja izdelan z upoštevanjem vseh dobrih praks in ustreznih rešitev, ki zagotavljajo visoko stopnjo informacijske varnosti.
Ker je informacijska varnost sistema odvisna od treh dejavnikov: okolja, informacijskega sistema in uporabnika je tudi skrb za njegovo varnost porazdeljena med tri glavne deležnike: informacijskega okolja (v konkretnem primeru ga v imenu naročnika zagotavlja MJU-DEUP), izvajalca, naročnika in uporabnika sistema.

Izvajalec lahko skladnost z zahtevami standarda ISO 27001 in 27002 zagotovi le v poglavjih oziroma delih, ki se neposredno nanašajo/navezujejo na aplikacijsko programsko opremo. To so predvsem poglavja o:

- skladnost (z zakonodajo, predpisi, standardi) (poglavje 15),
- zaščiti pred zlonamerno kodo (poglavje 10.4),

- nadzoru dostopa (poglavje 11),
- pravilna obdelava v aplikacijah (poglavje 12).

3.1.1.6 Nadzor informacijskih sistemov

Naročnik v dodatni dokumentaciji [1] predpisuje orodje IBM APP Scanner s katerim bo opravil varnostni pregled delovanja spletnih aplikativnih vmesnikov.

3.1.2 Infrastrukturna varnostna tveganja

Potrebno se je zavedati, da samo odprava opredeljenih varnostnih tveganj nikakor ni dovolj. Potrebno je zagotoviti tudi odpravo potencialnih ranljivosti zaradi: socialnega inženiringa, okvare ali izgube podatkov zaradi operativnih ali proceduralnih napak, naključnega razkritja, operacijskega sistema strežnika gostitelja, relacijske baze in transportne poti, arhitekturnih in infrastrukturnih nedoslednosti ali pomanjkljivosti. Izvajalec pri tem lahko sodeluje s predlogi in svetovanjem, vendar izvedba teh protiukrepov presega okvirje projekta razvoja informacijskega sistema eZapori.

3.1.2.1 Pristop - varnost podatkovnega toka

Z uporabo primerne tehnologije (SSL in TLS) bo zagotovljena enkripcija občutljivih podatkov na vseh delih IS eZapori (dostopnih tako znotraj IS eZapori, kot tudi preko intra/inter-neta), kjer prihaja do prenosa podatkov (kot na primer: pretok uporabniških imen in gesel, posredovanje osebnih podatkov, posredovanje drugih podatkov preko Internetnega omrežja med zunanjimi uporabniki eZapori in naročnikom, pretok pomembnih sistemskih/konfiguracijskih podatkov).

3.1.2.2 Javansko izvajalno okolje

Ker gre v primeru IS eZapori s stališča uporabniškega dostopa in arhitekture za spletno rešitev in pripadajoče spletne strukture podatkovne izmenjave, so bila pri pripravi rešitve in izbiri tehnologije upoštevane ključne ranljivosti spletnih aplikacij, pri čemer so bili uporabljeni podatki za leto 2010. Kot odgovor na ključne ranljivosti so bile podane ustrezne varnostne kontrole, ki bodo celovito (od arhitekture do kode) vključene v rešitev IS eZapori.

Nadzor po ISO27001: A.10.4 – Zaščita pred zlonamerno kodo

Standard ISO 27001 v poglavju 10.4 dodatka A obravnava kontrole za izvedbo zaščite pred zlonamerno in prenosno kodo in sicer:

- **A.10.4.1 Nadzor pred zlonamerno kodo**; uvesti in izvajati je potrebno ustrezne postopke in ozaveščanje uporabnikov za odkrivanje, preprečevanje in nadzor okrevanja za področje zaščite pred zlonamerno kodo.
- **A.10.4.2 Nadzor nad "mobilno" kodo**; kadar je dovoljena uporaba mobilne (prenosne) kode, se s konfiguracijo zagotovi, da pooblaščena mobilna koda deluje v skladu z jasno opredeljeno varnostno politiko. Nepooblaščeni mobilni kodi, je potrebno preprečiti izvršitev.

3.1.3 Varnostna tveganja spletnih aplikacij

Na spletni strani neprofitne organizacije OWASP (Open Web Application Security Project – https://www.owasp.org/index.php/Main_Page) je objavljenih 10 najpogosteje izkoriščanih ranljivosti spletnih aplikacij in spletnih storitev v letu 2010:

- A1: Vstavljanje (Injection),
- A2: Križno izvajanje skript (Cross-Site Scripting – XSS),
- A3: Prekinjeno razpoznavanje in upravljanje s sejami (Broken Authentication and Session Management),

- A4: Sklic na nevarne neposredne predmete (Insecure Direct Object References),
- A5: Medspletno ponarejanje zahtev (Cross-Site Request Forgery - CSRF)),
- A6: Nepravilne varnostne nastavitve (Security Misconfiguration),
- A7: Ranljivost kriptirane hrambe (Insecure Cryptographic Storage),
- A8: Napaka pri omejevanju dostopa do spletne strani (Failure to Restrict URL Access),
- A9: Neustrezno varovanje transportnega sloja (Insufficient Transport Layer Protection),
- A10: Nepreverjene preusmeritve in posredovanja (Unvalidated Redirects and Forwards).

V nadaljevanju so navedene ranljivosti in opisani protiukrepi za znižanje njihove učinkovitosti. Uporabili se bodo le protiukrepi, za katere se bo odločil naročnik ali izvajalec.

3.1.3.1 Vstavljanje (Injection)

Pri vstavljanju (ang. Injection) gre za napad, kjer so nezaupanja vredni podatki poslani interpreterju oziroma tolmaču kot ukaz ali poizvedba. Podatki napadalca lahko prelisičijo interpreter na način, da ta izvede neželen ukaz ali omogoči neavtoriziran dostop do podatkov.

Za namene zmanjševanja tveganj, povezanih z vstavljanjem, je bila uporabljena večnivojska arhitektura oziroma zgradba. Ta namreč po eni strani zmanjšuje razdrobljenost med posameznimi komponentami sistema, zvišuje jasnost vmesnikov in odgovornosti, po drugi pa predstavlja predpogoj za porazdeljeno procesiranje in več-nivojsko sistemsko arhitekturo. S tem se povečuje tako varnost izvajanja transakcij, kot njihova odzivnost v visoko obremenjenem omrežju.

Tu se vse SQL poizvedbe izvajajo na strežniku, kar pomeni, da posledično ni mogoče poslati nezaupanja vrednih podatkov tolmaču kot ukaz ali poizvedbo. Poleg tega so SQL stavki že vnaprej pripravljeni in se po potrebi lahko dodajajo le parametri (tu ni prisotnih SQL nizov). Za to se uporablja JDBC PreparedStatement. Poleg tega ni neposredne povezave na podatkovno bazo, kjer se nahajajo osebni podatki iz povezanih virov.

3.1.3.2 Križno izvajanje skript (XSS Cross site scripting)

Pri križnem izvajanju skript (ang. Cross Site Scripting - XSS) gre za izkoriščanje ranljivosti spletnih strani (obrazcev) z vrivanjem zlonamerne kode napisane v skriptnem jeziku, ki se izvede na strani odjemalca (obiskovalca spletne strani), z namenom kraje piškotkov, lažnega predstavljanja, vrinjenja besedil, novic iz zunanjih spletnih strani. Do tega napada pride zaradi tega, ker aplikacija sprejme nezaupanja vredne podatke in jih pošlje spletnemu brskalniku brez ustreznega preverjanja.

Za namene zmanjševanja tveganj, povezanih s križnim izvajanjem skript, so bila uporabljena digitalna potrdila (certifikati) med aplikacijo in strežniki virov. S tem je bilo preprečeno lažno predstavljanje na nivoju aplikacija – strežniki. Poleg tega se tu preverja veljavnost digitalnih potrdil in se uporabljajo samo sejni piškoti z omejeno veljavnostjo. Uporabniki se bodo na spletne storitve lahko prijavljali z digitalnimi potrdili, kar bo zmanjšalo možnost lažnega razpoznavanja.

3.1.3.3 Prekinjeno razpoznavanje in upravljanje s sejami (Broken authentication and session management)

Vzrok za prekinjanja postopka razpoznavanja in upravljanja s sejami (ang. Broken Authentication and Session Management) so aplikacijske funkcionalnosti, ki se nanašajo na avtentikacijo in upravljanje s sejami, ki niso pravilno implementirane. To napadalcem omogoča napad na gesla, ključe, sejne žetone (token) ali izkoriščanje drugih lukenj z namenom prevzemanja digitalnih identitet.

Za namene zmanjševanja tveganj, povezanih s prekinjanjem razpoznavanja in upravljanja s sejami, je bilo upravljanje s sejami prepuščeno skupku knjižnic za programski sistem. Za varno avtentikacijo in avtorizacijo (torej dostopne pravice) skrbi varnostni sistem Spring Security. Za varnost na sejah skrbi spletni strežnik WebLogic. Kot varnostna kontrola za preprečevanje prestrezanja prometa je bila tu uporabljena varna povezava HTTPS (digitalna potrdila).

3.1.3.4 Sklic na nevarne neposredne predmete (Direct object references)

Neposredni sklic na predmet (ang. Direct Object References) se pojavi, ko razvijalec izpostavi referenco na interni predmet izvajanja, kot je datoteka, mapa ali ključ podatkovne baze. Brez ustreznega nadzora dostopa ali drugih varnostnih kontrol, lahko napadalec manipulira s temi referencami na način, da si pridobi nepooblaščen dostop do podatkov.

Za namene zmanjševanja tveganj, povezanih s sklicevanjem na nevarne neposredne predmete oziroma ang. Insecure Direct Object References, je bila uporabljena varnostna aplikacijska logika. Ta predstavlja temelj obrambe zoper te napade. Dodatno varnost tu nudita še varnostni sistem Spring Security, ki omejuje uporabniške vloge in natančna poslovna logika. Na ta način se natančno ve, kateri uporabnik nastopa v kateri vlogi (vnaprej se določi dostop do transakcij).

3.1.3.5 Medspletno ponarejanje zahtev (Cross site request forgery- CSRF)

Za razliko od križnega izvajanja skript (XSS), ki zlorablja zaupanje uporabnika do strežnika oziroma spletne strani, medspletno ponarejanje zahtev (ang. Cross Site Request Forgery) zlorablja zaupanje strežnika do uporabnika. Zaupanje na tej relaciji je vedno pogojeno z avtentikacijo in sejo. Po uspešno opravljeni avtentikaciji se seja navadno vzpostavi s pomočjo SessionID-jev in/ali piškotkov (cookies). Predpogoj za uspešno izvedeno križno ponarejanje zahtevkov je seveda predhodno vzpostavljena, aktivna seja. Tu mora biti uporabnik prijavljen v spletno aplikacijo. Napad med-spletnega ponarejanja zahtev prisili prijavljen žrtvin spletni brskalnik, da pošlje ponarejeno spletno zahtevo, vključno z žrtvinim sejnim piškotom in katerimikoli drugimi samodejnimi avtentikacijskimi informacijami, na ranljivo spletno aplikacijo. To napadalcem omogoči, da žrtvin brskalnik prisilijo h generiranju zahtevkov z namenom, da ranljivo aplikacijo prepričajo, ga tu gre za legitimne zahtevke.

Za namene zmanjševanja tveganj, povezanih z med-spletnim ponarejanjem zahtev, je bil vzpostavljen protokol HTTPS, ki nudi zaščito na povezavi med brskalnikom in strežnikom. S tem se lahko prepreči okoli 90 odstotkov tovrstnih napadov.

Za zmanjševanje preostalih tveganj medsebojnega ponarejanja zahtev, kot so npr. ranljivi in ne posodobljeni spletni brskalniki, neustrezna protivirusna zaščita, ne posodobljen in/ali zastarel operacijski sistem in podobno, je zadolžen naročnik oziroma upravljavci infrastrukture na Ministrstvu za javno upravo ali Ministrstvu za pravosodje. Na njih izvajalec namreč nima vpliva in za njih ni odgovoren.

3.1.3.6 Nepravilne varnostne nastavitve (Security Misconfiguration)

Dobra varnost zahteva natančno opredeljene in vpeljane varnostne nastavitve. To velja za aplikacije, zbirke knjižic, aplikacijski strežnik, spletni strežnik, podatkovni strežnik in platformo. Vse te nastavitve je zato potrebno natančno opredeliti, implementirati in vzdrževati. To vključuje nameščanje varnostnih popravkov za programsko opremo, vključno z zbirkami knjižnic, ki jih

aplikacija uporablja. V nasprotnem primeru lahko pride do napada zaradi nepravilne varnostne nastavitve. Zmanjševanje teh tveganj je v izključni pristojnosti naročnika. Na njih izvajalec nima vpliva in za njih ni odgovoren.

3.1.3.7 »Ranljiva« šifrirana baza podatkov (Insecure Cryptographic Storage)

Številne spletne aplikacije ne ščitijo občutljivih podatkov, kot so na primer osebni podatki in to kljub uporabi šifrirnega ali zgoščevalnega algoritma, na ustrezen način. To je lahko tako posledica neuspešnega šifriranja podatkov kot neustrezne postavitve šifrirne platforme (ang. Insecure Cryptographic Storage).

Zaradi ranljivosti ali neustreznih nastavitev lahko potencialni napadalec ukrade ali ponaredi slabo varovane podatke. To posledično privede do kraje osebnih podatkov.

Za namene zmanjševanja tveganj, povezanih z ranljivo šifrirano bazo podatkov, je potrebno uporabljati varna in zaupanja vredna digitalna potrdila, kar naročnik zagotavlja z izključno uporabo javnih, veljavnih digitalnih potrdil, kot tudi lastno infrastrukturo javne CA. Ključno vlogo igra tu še popolna in ažurna sistemska in tehnična dokumentacija. Zmanjševanje teh tveganj je v izključni pristojnosti naročnika. Na njih izvajalec namreč nima vpliva in za njih ni odgovoren.

3.1.3.8 Napaka pri omejevanju dostopa do URL (Failure to Restrict URL Access)

Številne spletne aplikacije preverjajo URL dostopne pravice preden prikažejo zaščitene povezave in gumbe. Kljub temu morajo aplikacije opravljati podobna preverjanja dostopni kontrol vsakokrat, ko se dostopa do teh strani. V nasprotnem primeru lahko napadalec ponaredi URL in si s tem pridobi dostop do »skritih« vsebin. Tu gre za napad omejevanja dostopa do URL (Failure to Restrict URL Access).

Za namene zmanjševanja tveganj, povezanih z napakami pri omejevanju dostopa do URL naslovov, je bila uporabljena varnostna aplikativna logika, enako kot je opisano v poglavju 3.1.3.4).

3.1.3.9 Neustrezno varovanje transportnega sloja (Insufficient Transport Layer Protection)

Aplikacije pogosto naredijo napako pri avtentikaciji, šifriranju in varovanju zaupnosti in celovitosti občutljivega mrežnega prometa. To je pogosto posledica uporabe slabih šifrirnih algoritmov, uporaba pretečenih ali neustreznih certifikatov oziroma digitalnih potrdil ali njihova neustrezna uporaba. Tu gre za napad neustreznega varovanja transportnega sloja (Insufficient Transport Layer Protection).

Zmanjševanje tega tveganja je v izključni pristojnosti naročnika oziroma Ministrstva za javno upravo. Na njih izvajalec nima vpliva in za njih ni odgovoren.

3.1.3.10 Nepreverjene preusmeritve in posredovanja (Unvalidated Redirects and Forwards)

Spletne aplikacije uporabnike pogosto preusmerijo ali prenesejo na druge strani ali spletne strani. Pri tem uporabljajo nezaupanja vredne podatke za določanje končnih strani. Brez ustreznega preverjanja lahko napadalci žrtev preusmerijo na lažne ali zlonamerne spletne strani. To lahko zlorabijo celo za neavtoriziran dostop do strani. Tu gre za napad nepreverjene preusmeritve in posredovanja.

Za namene zmanjševanja tveganj, povezanih z nepreverjenimi preusmeritvami in posredovanji (ang. Unvalidated Redirects and Forwards), je bila uporabljena aplikativna logika in varnostni sistem Spring

Secirity, (enako kot v poglavju 3.1.3.4). Za preprečitev napada se mora namreč pravilno izvesti tako razpoznavanje kot avtorizacija uporabnika. Poleg tega se vsi zahtevki na spletni strani preverijo. Čeprav uporabnik neposredno vnese URL naslov, se vedno samodejno preverita tako razpoznavanje kot avtorizacija.

3.1.4 Varnostna tveganja Oracle APEX

V nadaljevanju so ločeno za tehnologijo Oracle APEX opredeljena varnostna tveganja in protiukrepi za njihovo odpravo. Uporabili se bodo le protiukrepi, za katere se bo odločil naročnik ali izvajalec.

Vseh, v nadaljevanju predstavljenih APEX varnostnih izpostavljenosti in ranljivosti, se lahko izognemo z natančno konfiguracijo. Še vedno pa obstaja veliko potencialnih varnostnih izpostavljenosti, ki jih je potrebno preučiti, o njih razmisliti in jih, skladno s konfiguracijo informacijskega sistema, minimizirati. Obstaja več področij možne izpostavljenosti APEX:

- SQL Vstavljanje (SQL Injection) – varnostna grožnja z uporabo SQL konstruktov,
- Križno izvajanje skript (XSS Cross site scripting) – varnostna grožnja z izkoriščanjem posebnih znakov,
- Prisluškovanje (Eavesdropping) – prisluškovanje in pridobivanje vsebine podatkovnih paketov,
- Zavarovanje stanja seje (SSP Session State Protection) in Prirejanje spletnih naslovov (URL Tampering) - prepreči namerno ali nenamerno manipulacijo spletnih naslovov. Ob napačni konfiguraciji APEX, lahko končni uporabniki spremeni spletni APEX naslov in dostopa do podatkov zunaj področja načrtovane uporabe APEX.
- Virtual Private Database – omogoča večjo ločitev med varnostno in aplikacijsko logiko,
- Ranljivost iskalnika (Search Engine vulnerability) - Če iskalnik indeksira Oracle APEX spletno stran, so v rezultatih iskalnika objavljeni spletni naslovi z izpostavljenimi vrednostmi podatkov (»f?p«)
- Statistična izpostavljenost napotitelja (Referrer statistics exposure) - Če končni uporabnik klikne izven APEX strani, obstaja možnost, da spletni naslov napotitelja (spletna stran, ki neposredno zagotavlja promet) pošlje stare (APEX) vrednosti na naslov nove spletne strani,
- Podatkovni sesalniki (Hoover Bots) - napadalci lahko preko skript, ki posnemajo APEX transakcije, pridobijo (posesajo) izpostavljene Oracle podatke.

3.1.4.1 SQL Vstavljanje

SQL vstavljanje je varnostna grožnja, ki preko vnosa SQL konstruktov v vnosno polje, poskuša vstaviti ali sestaviti SQL predikatni stavek. Podobno kot križno vstavljanje tudi SQL vstavljanje ne zahteva posebnih pravic ali dostopa do aplikacije ali kode.

Rešitev za preprečevanje SQL vstavljanja je v uporabi vezanih spremenljivk. Poizvedbe za preprečevanje SQL vstavljanja tipično glasijo:

```
select "NR", "POS", "NAME"
from "#OWNER#"."TEAM"
where "POS"='PUBLIC'
and "NAME" like '%'||:P1_X||'%'
```

Ta rešitev se uporablja ne le za Application Express, temveč tudi za druga razvojna orodja, kot je Visual Basic in Java.

3.1.4.2 Križno izvajanje skript (XSS Cross site scripting)

Križno izvajanje skript (imenovano tudi XSS, Cross site scripting), je varnostna grožnja, ki izkorišča dinamično generirane spletne strani. V XSS napadu je spletni aplikaciji poslan scenarij, ki se aktivira, ko je prebran z uporabnikovim brskalnikom. Ko je enkrat aktiviran, lahko izvede krajo podatkov, vključno s poverilnicami spletne seje in preusmeri informacije na napadalca.

Za preprečevanje napadov križnega izvajanja se je potrebno izogibati posebnim znakom. V nastavitvah APEX to izvedemo preko nastavitev atributov »Display as text (escape special characters)«

3.1.4.3 Prisluškovanje

Izraz prisluškovanje se nanaša na neodrejeno število uporabljenih tehnik za nepooblaščeno pregledovanje prometa, ki se pojavlja znotraj veljavne http seje. Prisluškovanje je mogoče izvajati z zlonamerno programsko opremo (trojanski konji), s prestrezanjem prometa na delovni postaji, s prestrezniki paketnega prometa (packett sniffers), ki lahko delujejo kjerkoli na komunikacijski poti (končne točke ali omrežna vozlišča).

Najboljša obramba pred prisluškovanjem katere koli vrste, je vzpostavitev varne povezave med spletnim brskalnikom in Apex aplikacijskim strežnikom. Za vzpostavitev zaščite pred prisluškovanjem bo na vseh, z naročnikove strani identificiranih mestih (posebej pr prijava, pregled osebnih ali občutljivih osebnih podatkov, ipd) uvedena SSL ali TLS na povezavo HTTP – omogočena bo varna povezava HTTPS. Tudi vse Apex posredovalne sheme podpirajo HTTPS. Apex bo nastavljen z zahtevo, da so vse njegove identificirane povezave varne povezave.

3.1.4.4 Zavarovanje stanja seje (SSP, Session State Protection) in prirejanje spletnih naslovov (URL Tampering)

Zavarovanje statusa seje (Session države Protection, SSP), je način varovanja podatkov, shranjenih v seji neposrednega uporabnika, pred nepooblaščeno manipulacijo. Z uporabo SSP mehanizmov je aplikacija sposobna odkriti, ali uporabnik naključno ali namerno manipulira s spletnimi naslovi, v poskusu, da pridobi dostop ali spremeni sejo v posamezni točki.

Ranljivosti se bomo izognili preko omogočanja osnovne nastavitve SSP znotraj čarovnika:

- Application Attributes->Security Atributes oziroma
- Shared Components -> Session State Protection

ter dodatno preko nastavitev vrednosti štirih atributov: Page access protection, Application item protection, Page data entry item protection, Page display-only item protection).

Nedovoljeni poseg preko prirejanja spletnih naslovov se nanaša na kateri koli poseg, katerega namen je, preko spremenjene vsebine spletnega naslova, pridobiti pravice ali informacije, ki preko veljavne uporabe aplikacije in dostopa do APEX spletnih strani niso na voljo. APEX je preko svojega osnovnega načina naslavljanja spletnih vsebin (f?p=&APP_ID.:1:::::P1_EMPID:12) na takšne napade še posebej občutljiv.

Obstajajo štirje osnovni načini upravljanja s spletnimi naslovi znotraj APEX (posredovanje zahtev (Proxying Requests), preusmeritev (Location Redirect), uporaba okvirjev (Using Frames), Apche mod_rewrite)) ki so na voljo razvijalcu ali uporabniku in omogočajo učinkovito zakrivanje podrobne vsebine spletnih naslovov.

3.1.4.5 Virtual Private Database

Ena od prednosti uporabe APEX za oblikovanje in izvajanje aplikacij je sposobnost za izvajanje politike nadzor dostopa na ravni podatkovne baze in ne le na ravni aplikacije. V primeru uporabe relacijske baze podatkov Oracle Enterprise Edition (kar pri IS eZapori je primer) je omogočena uporaba Virtual Private Database (VPD) funkcija, ki je poznana tudi kot podrobnejši nadzor dostopa (Fine Grain Access Control, ali FGAC).

Uporaba VPD omogoča:

- ločitev varnostne in aplikativne logike,
- višjo raven revizijske sledljivosti podatkovnim spremembam,
- enostavnejše spreminjanje varnostne logike (uporaba kontekstov),
- zaščita podatkov neodvisno od primera dostopa,
- enostavnejše vzdrževanje.

Vse naštete in tudi druge (napredne) lastnosti, ki jih prinaša VPD v primeru IS eZapori govorijo v prid njegovi izbiri.

3.1.4.6 Ranljivosti iskalnika

Če iskalnik (Google ali podobni) indeksira APEX zbirke podatkov lahko pride do razkritja zaupnih podatkov v javnosti. Ob uporabi "inurl:" iskalne funkcije lahko prikaz rezultatov omejimo na APEX strani kjer spletni naslov vsebuje niz "f p =?".

Opisana izpostavljenost ni omejena samo na Google. Mnogi iskalniki (predvsem zlonamerni) ne spoštujejo "nofollow" oznake na straneh. Upravljavec relacijske baza (DBA) mora vedno zagotoviti, da so vsi podatki in nastavitve znotraj APEX shranjeni v z geslom zavarovane imenike, in tako zaščitene pred iskalniki. Dovoljenja tipa 700 ali 770 na teh imenikih, bodo poskrbela za takšno izpostavljenost.

3.1.4.7 Podatkovni sesalci

Vsi ali del podatkov, dostopnih prek uporabe APEX spletnih aplikacij, ki niso ustrezno varnostno upravljani (zavarovani), so lahko kot tarča napadalcev prekopirani v drugo Oracle podatkovno zbirko. Znan je primer vdora in prepisa bralnih navad 260.000 ameriških državljanov iz spletne strani Amazon.com.

Znotraj Oracle Application Express (APEX) 4.1 sta dodana dva nova nabora atributov za povišanje stopnje varnostni spletnega brskanja: Cache (predpomnilnik) in Embed in Frames (vgrajeni okvirji). sistema eZapori.

3.1.4.8 Predpomnilnik (CACHE)

Predpomnilnik (CACHE) omogoča brskalniku shraniti vsebino strani ali aplikacije v hitri predpomnilnik (cache) v pomnilniku in na disku osebnega računalnika. Če uporabnik pritisne gumb za brskalnik nazaj, bo stran običajno mogoče naložiti iz predpomnilnika, ne iz strežnika. Če je predpomnilnik onemogočen, je to navodilo brskalniku, naj vsebine strani ne hrani lokalno, temveč jo vedno na novo zahteva od strežnika.

Z vidika varnosti je potrebno hitri predpomnilnik za vse strani s poslovnimi, osebnimi ali občutljivimi osebnimi podatki onemogočiti, tako da brskalnik teh podatkov ne shranjuje in vedno zahteva spremembe spletnih strani od strežnika.

3.1.4.9 Prikaz v okvirjih (Embed in Frames)

Prikaz strani v okvirih je mogoče zlorabiti z napadi tipa »clickjacking«. To so tipi napada, ko napadalec uporablja več plasti ter preusmerja uporabnika na drugo povezavo ali drugo okno / drugo stran, ko so bili nameravajo kliknite na vrhu strani ravni. Tako napadalec ugrablja klike in jih usmerja na drugo stran.

Uporaba tega atributa omogoča nadzor, kdaj brskalnik lahko prikaže vsebino znotraj okvirjev in sicer:

- Prepovej (Deny): Strani ni mogoče prikazati v okvirju, ne glede na mesto.
- Dovoli iz istega izvora (Allow from same origin): stran je lahko prikazana samo v okvirju za istega izvora kot sama stran.
- Dovoli (Allow): stran je lahko prikazana v katerem koli okvirju.

3.1.5 Varnostna tveganja Oracle FORMS

V nadaljevanju so ločeno za tehnologijo Oracle FORMS opredeljena varnostna tveganja in protiukrepi za njihovo odpravo.

Podatki o ranljivostih, ki jih predstavljamo v nadaljevanju so povzeti po spletni strani MITRE CVE (http://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-5102/version_id-22585/Oracle-Forms-10G.html). Podatki so privzeti iz nacionalne baze podatkov (National Vulnerability Database, NVD; http://nvd.nist.gov/), ki jo preko XML virov zagotavlja ameriški Nacionalni inštitut za standarde in tehnologijo (National Institute of Standards and Technology, NIST, http://www.nist.gov/index.html).

V nadaljevanju so predstavljene ranljivosti, ki so bile ugotovljene na verziji Oracle Forms 10g in z nekateirmi omejitvami po razpoložljivih podatkih ob neprevidnem programiranju veljajo tudi v višjih verzijah.

Oznaka: CVE-2005-3207	
Tip Ranljivosti:	ohromitev storitve (DoS)
Datum objave:	14. 10. 2005
Datum zadnje posodobitve:	05. 09. 2008
Podrobnosti o ranljivosti:	Strežniški programi (f90servlet) v Oracle Forms 4.5.10.22 omogoča tip napada ohromitev storitve (DoS). Oddaljeni napadalec preko parametra userid, ki vsebuje ukaz STOP, povzroči zaustavitev storitve TNS listener.

Oznaka: CVE-2005-2372

Tip Ranljivosti:	izvršna koda
Datum objave:	26. 07. 2005
Datum zadnje posodobitve:	05. 09. 2008
Podrobnosti o ranljivosti:	Oracle Forms od verzije 4.5 do 10g zažene izvršno kodo iz poljubne mape in jo izvaja kot Oracle ali sistemski uporabnik, kar omogoča napadalcu da preko preko prenosa zlonarmerne .fmx datoteke in ob navajanju absolutne poti do datoteke v argumentu (1) form ali (2) module parameters za strežniški program (f90servlet).

Oznaka: CVE-2005-1178	
Tip Ranljivosti:	izvršna koda sql
Datum objave:	02. 05. 2005
Datum zadnje posodobitve:	05. 09. 2008
Podrobnosti o ranljivosti:	Ranljivost SQL injection v Oracle Forms 10g omogoča oddaljenemu napadalcu izvajanje poljubnega SQL ukaza preko funkcije Query/Where.

3.2 Zaključek

Vsi napori pri pripravi projektne dokumentacije, ter kasnejše izvedbe znotraj projekta eZapori, potekajo s ciljem upoštevanja veljavne zakonodaje, priporočil varstva osebnih podatkov, mednarodnih standardov in načel dobre prakse pri razvoju aplikacijske programske opreme. To bo v največji meri zagotovilo varnost informacijskega sistema, ki pa je le člen v verigi celovite varnosti informacijske rešitve. Zato bo varnost v delovanju (obratovanju, uporabi) končnega izdelka skoraj v celoti odvisna od naročnika in uporabnika.

Končni izdelek je namenjen v izključno notranjo uporabo znotraj privatnega, dostopno in vsebinsko varovanega transportnega omrežja in infrastrukturnega centra – HKOM, MJU-PDC in MP-PDC. Zato je verjetnost, da bo informacijski sistem podvržen najmodernejšim in najbolj proaktivnim oblikam in poskusom vdorov, dostopa do podatkov in težnjam k prekinitvi razpoložljivosti ali delovanja relativno majhna.
Potrebno se je zavedati, da samo odprava opredeljenih varnostnih tveganj nikakor ni dovolj. Potrebno je zagotoviti tudi odpravo potencialnih ranljivosti zaradi: socialnega inženiringa, okvare ali izgube podatkov zaradi operativnih ali proceduralnih napak, naključnega razkritja, operacijskega sistema strežnika gostitelja, relacijske baze in transportne poti, arhitekturnih in infrastrukturnih nedoslednosti ali pomanjkljivosti. Zato je potrebno neprekinjeno spremljanje vseh ranljivosti, posodabljanje sistemske programske opreme in informacijske rešitve, kot tudi zagotavljanje najboljše infrastrukturne podpore.