



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA PRAVOSODJE



UČINKOVITO
PRAVOSODJE



EVROPSKA UNIJA
EVROPSKI
SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST



Razvoj novega informacijskega sistema centralne kazenske evidence

Sistemsko-tehnična dokumentacija Arhitektura sistema

Verzija 1.0

Naročnik:	Ministrstvo za pravosodje
Datum verzije dokumenta:	19.05.2023
Verzija dokumenta:	1.0
Verzija aplikacije:	1.0 (1.0.18.2)
Avtor:	SRC d. o. o.
Stopnja zaupnosti:	Dokument za notranjo uporabo



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA PRAVOSODJE



UČINKOVITO
PRAVOSODJE



EVROPSKA UNIJA
EVROPSKI
SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST



ZGODOVINA DOKUMENTA

Dokument opredeljuje arhitekturo sistema CKE s stališča tehnološke arhitekture, varnosti, nadzora, revizijske sled in uporabljenih standardov.

Datum	Verzija	Opis	Avtor
19.05.2023	1.0	Vzpostavitev dokumenta	SRC d.o.o.



VSEBINA

1.	Uvod	4
2.	Tehnološka arhitektura	4
2.1	Predpostavke pri izvedbi rešitve IS CKE	4
2.2	Tehnološka aplikativna arhitektura	5
2.2.1	Predstavitveni sloj	4
2.2.2	Poslovni sloj	4
2.2.3	Storitveni sloj	4
2.2.4	Podatkovni sloj	4
2.3	Gradniki sistema	5
2.3.1	Docker vsebniki	5
2.3.2	Spletne končne točke	5
2.3.3	Podatkovna baza	6
2.4	Infrastrukturni pogled	7
2.4.1	Topologija sistema	7
2.4.2	Mrežne povezave	5
2.4.3	Nameščanje sistema	4
3.	Navezava na zunanje sisteme	4
3.1	Laurentius (VSRS)	4
3.2	ECRIS	4
3.3	ZUSERVIS - SPLETNI SERVIS SISTEMA IS CKE	5
3.4	CRP (MNZ)	5
3.5	PRS (Ajpes)	5
4.	Varnost	5
4.1	Uporabniki sistema	5
4.2	Upravljanje z identitetami in dostopi uporabnika	5
4.2.1	Identifikacija uporabnikov z uporabo gradnika SI-CAS	6
4.2.2	Avtorizacija uporabnikov	6
4.2.3	Avtentikacija in avtorizacija odjemalcev zuServis-a	6
4.2.4	Gradniki infrastrukture	6
4.2.5	Delovanje	7
4.3	Kontrola pristopa	8
4.3.1	Kontrola pristopa na nivoju uporabniškega vmesnika	9
4.3.2	Kontrola dostopa na nivoju podatkovne baze	9
4.4	Varovanje omrežnega prometa	9
5.	Nadzor in upravljanje sistema	9
5.1	Upravljanje sistema	9
5.2	Spremljanje delovanja sistema	9
5.3	Revizijska sled sistema	10
6.	Okolja	10
6.1	Okolja pri lastniku in upravljalcu centralne infrastrukture (MJU)	11
6.2	Okolja izvajalca (SRC)	11



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA PRAVOSODJE



UČINKOVITO
PRAVOSODJE



EVROPSKA UNIJA
EVROPSKI
SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST



7.	Uporabljeni standardi in tehnologije	12
7.1	Standardi in tehnologije Oracle podatkovne baze	13



1. UVOD

Izvajalec je za naročnika Ministrstvo za pravosodje razvil nov informacijski sistem Centralne kazenske evidence (IS CKE). Z razvojem novega sistema je naročnik pridobil nove, prenovljene in dopolnjene delovne procese in opravila sistema centralnih kazenskih evidenc.

Dokument »Arhitektura sistema« (PZI) je krovni dokument tehnične dokumentacije projekta »Razvoj novega informacijskega sistema centralne kazenske evidence«.

Podana je krovna slika rešitve z vidika več nivojev, kot je navedeno v nadaljevanju:

- poslovni nivo,
- tehnološki nivo,
- varnost,
- nadzor,
- revizijska sled.

Poslovni nivo podaja celovito vsebinsko sliko - izvedene procese znotraj IS CKE.

Tehnološki nivo podaja celovito sliko področij:

- aplikativne arhitekture sistema,
- arhitekture programskega izvajalnega okolja,
- arhitekture infrastrukture (strojna in mrežna oprema).

S stališča varnosti, nadzora in revizijske sledi so predstavljeni naslednji nivoji:

- poslovna varnost, nadzor in revizijska sled,
- aplikativna varnost, nadzor in revizijska sled,
- podatkovna varnost, nadzor in revizijska sled,
- infrastrukturna varnost, nadzor in revizijska sled.

Dokument podaja tudi opise uporabljenih poslovnih in tehnoloških standardov.

2. TEHNOLOŠKA ARHITEKTURA

2.1 PREDPOSTAVKE PRI IZVEDBI REŠITVE IS CKE

Tekom izvedbe rešitve IS CKE so bile upoštevane naslednje predpostavke:

- izvajalec ni skrbnik infrastrukture (mrežna in strojna oprema, programska izvajalna okolja),
- IS CKE je nameščen na infrastrukturo, ki je v upravljanju Ministrstva za javno upravo,
- tehnologije in gradniki so skladni z razpisno dokumentacijo ter GTZ (Generične tehnološke zahteve),
- za avtentikacijo uporabnikov so uporabljeni mehanizmi, ki zagotavljajo visoko stopnjo zaupanja (digitalno potrdilo, SMSPass). Uporabljena sta bila skupna gradnika SI-PASS in Varnostna Shema,
- končni uporabniki uporabljajo verzije spletnih brskalnikov (Edge, Firefox, Chrome, Safari), ki so trenutno podprte s strani proizvajalca,
- za vizualizacijo prikaza na predstavitvenem sloju aplikacij se uporablja ogrodje Angular,
- minimalna priporočljiva zaslonska ločljivost je 1280 x 1024

Poleg zgornjih predpostavk so bili uporabljeni tudi naslednji pristopi:



- uporabljena je bila arhitektura mikrororitev ter tehnologija .Net Core,
- uporablja se Oracle podatkovni strežnik 19c,
- sistem se izvaja na platformi, ki podpira Docker vsebnike (Docker Swarm),
- rešitev IS CKE je dostopna samo znotraj omrežja državnih organov (HKOM).

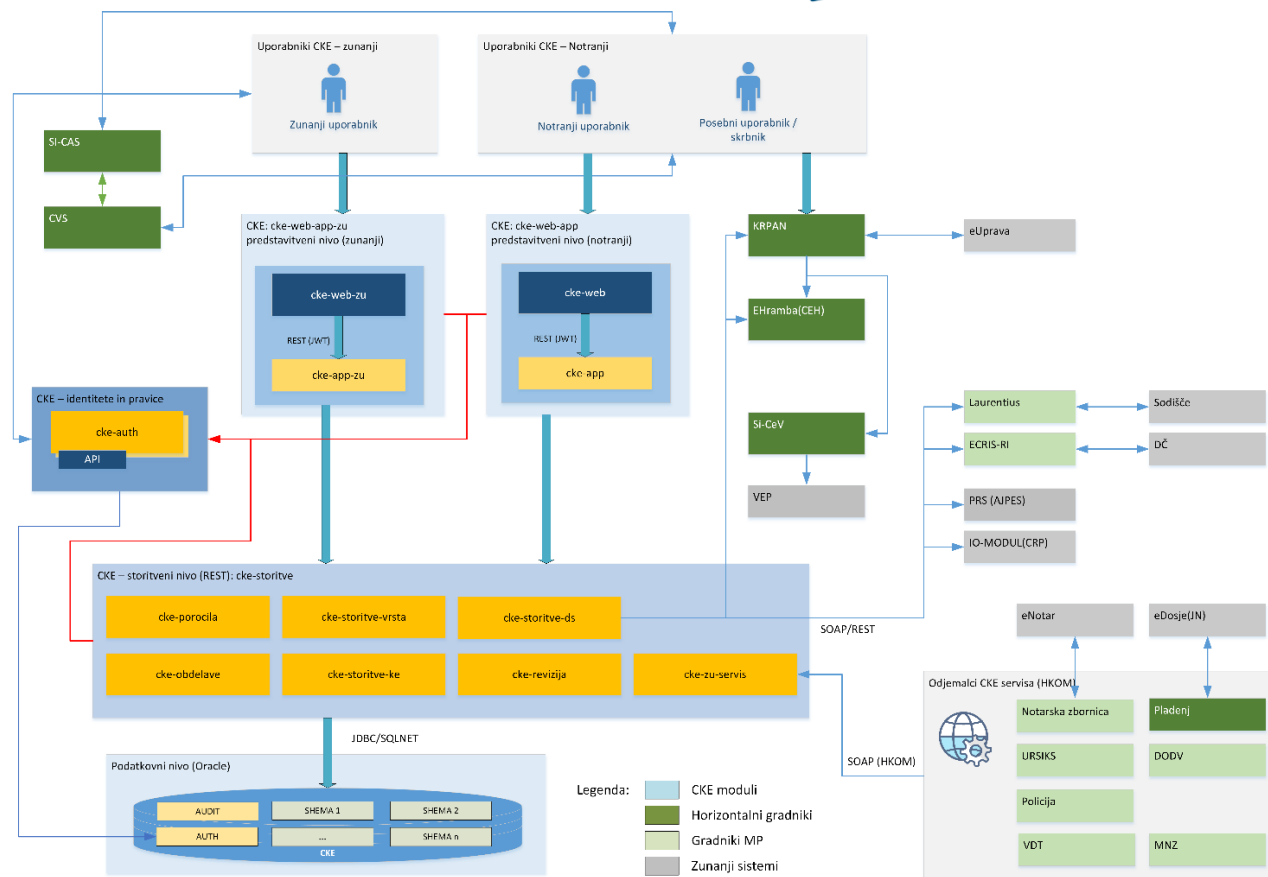
2.2 TEHNOLOŠKA APLIKATIVNA ARHITEKTURA

Tehnološka arhitektura IS CKE temelji na sodobnih pristopih, ki se trenutno uporabljajo za sisteme elektronskega poslovanja ter spletnih portalov. Ti arhitekturni pristopi se nagibajo v smeri arhitekture mikrororitev, ki si jih lahko predstavljamo kot zbirko neodvisnih funkcionalnosti, ki pa skupaj tvorijo enoten sistem.

Arhitektura sistema je zasnovana v več slojih, ki predvideva porazdelitev mikrororitev na različne sloje glede na vrste in namen mikrororitve. Tako se predvidevajo sledeči sloji:

- prezentacijski,
- poslovni,
- storitveni,
- podatkovni.

V arhitekturo so vključeni tudi elementi, ki so prisotni v vseh slojih arhitekture. Ti elementi skrbijo za varnost in nadzor dostopov do sistema, spremljanje in nadzor delovanja ter beleženje dogodkov vključno z ustvarjanjem revizijske sledi. Prav tako je vključena možnost uporabe zunanjih vmesnikov/storitev. Tehnološko arhitekturo prikazuje spodnja slika.



Slika 1: Tehnološka aplikativna arhitektura sistema IS CKE



Izvedba je zasnovana tako, da je lahko posamezen gradnik ena ali več mikrorstitev, odvisno od namestitvenega modela, ki ga bo uporabil naročnik oz. upravljalec izvajalnega okolja. Glede na trenutno predvideno okolje s strani MJUja - Docker Swarm, predlagamo eno mikrorstitev/gradnik.

2.2.1 Predstavitveni sloj

Predstavitveni sloj predstavlja vmesnik, ki omogoča interakcijo med uporabnikom in zalednim sistemom. V sistemu IS CKE sestavljajo predstavitveni nivo trije logični moduli in sicer:

- **spletna aplikacija za notranje uporabnike:** izvedena je kot Single Page Application (SPA) z ogrodjem Angular in je namenjena uporabnikom IS CKE v okviru MP,
- **spletna aplikacija za registrirane zunanje uporabnike:** izvedena je kot SPA z ogrodjem Angular in je namenjena uporabnikom izven MP, ki dostopajo do sistema zgolj na podlagi povpraševanj,
- **spletna aplikacija v okviru IS za delo z dokumentarnim gradivom:** del funkcionalnosti uporabniškega vmesnika se izvaja znotraj IS za delo z dokumentarnim gradivom KRPAN, ki ga upravlja MJU.

2.2.2 Poslovni sloj

Poslovni sloj predstavlja vmesnik, ki zagotavlja poslovno logiko posameznim spletnim aplikacijam prezentacijskega sloja. Sistem IS CKE v poslovnem sloju sestavljata naslednja gradnika:

- gradnik **cke-app** zagotavlja spletne storitve, ki se bodo uporabljale znotraj spletne aplikacije prezentacijskega sloja notranjim uporabnikom,
- gradnik **cke-app-zu** zagotavlja spletne storitve, ki se bodo uporabljale znotraj spletne aplikacije prezentacijskega sloja za zunanje uporabnike.

2.2.3 Storitveni sloj

Na storitvenem sloju se nahaja več gradnikov, ki zagotavljajo različne vrste storitev. Tako ločimo:

- poslovne storitve, namenjene spletnim aplikacijam,
- integracijske storitve, ter
- podporne storitve.

Poslovne storitve zagotavljajo izvajanje poslovnih opravil znotraj sistema. Gradniki **cke-storitve-ke**, **cke-storitve-vrsta**, **cke-storitve-ds** in **cke-revizija** zagotavljajo poslovno logiko, ki se bo tipično uporabila znotraj spletnih storitev za potrebe prezentacijskega sloja. Storitve prav tako s pomočjo podatkovnega sloja zagotavljajo persistenco podatkov.

Podporna storitev **cke-porocila** je namenja pripravi izpisov dokumentov ter poslovni statistiki, storitve cke-obdelave pa podpora periodičnim opravilom.

Ločeno od storitev, ki zagotavljajo delovanje spletnim aplikacijam je zasnovana storitev **cke-zu-servis**, ki zagotavlja SOAP vmesnik do sistema IS CKE.

2.2.4 Podatkovni sloj

Podatkovni sloj nudi infrastrukturo za trajno shranjevanje podatkov brez izgub. Realiziran je na infrastrukturi Oracle Enterprise Edition 19c.



Podatkovne zbirke za aplikacijo so realizirane kot samostojne sheme znotraj fizične instance Oracle in iste zbirke podatkov CKE. Sheme so vzpostavljene glede na vsebinska področja sistema. Baza za beleženje dostopov, vpogledov in sprememb je realizirana kot ločena zbirka podatkov AUDIT.

Dostop do podatkovnih zbirk

Moduli sistema IS CKE se na podatkovno zbirko prijavljajo z namenskim uporabnikom, ki ima minimalen zadosten nabor pravic, ki aplikaciji še omogoča pravilno delovanje in izvrševanje poslovne logike. Vsak modul (gradnik) uporablja svojega namenskega baznega uporabnika.

Za dostop do relacijske podatkovne baze in podatkov, ki se obdelujejo v poslovni logiki je uporabljen ustrezen ORACLE odjemalec glede na tehnologijo izvedbe poslovne logike (JDBC oz. ODP.NET Core). Za klice iz gradnikov poslovnega sloja je uporabljeno objektno-relacijsko mapiranje (ORM) v kombinaciji z baznimi procedurami.

2.3 GRADNIKI SISTEMA

2.3.1 Docker vsebniki

Sistem CKE sestavljajo naslednji Docker vsebniki namenjeni nameščanju:

Spletne aplikacije:

- **cke-web-app**: vsebuje spletno mesto **cke-web** in spletne storitve **cke-app**,
- **cke-web-app-zu**: vsebuje spletno mesto **cke-web-zu** in spletne storitve **cke-app-zu**,

Storitve:

- **cke-auth**: vsebuje avtorizacijski podsistem,
- **cke-storitve**: vsebuje naslednje storitve
 - cke-storitve-ke,
 - cke-storitve-vrsta,
 - cke-storitve-ds,
 - cke-obdelave,
 - cke-porocila,
 - cke-revizija,
 - cke-zu-servis

2.3.2 Spletne končne točke

V nadaljevanju so podane povezave spletnih naslov in gradnikov za produkcijsko okolje.

Spletno mesto cke.sigov.si

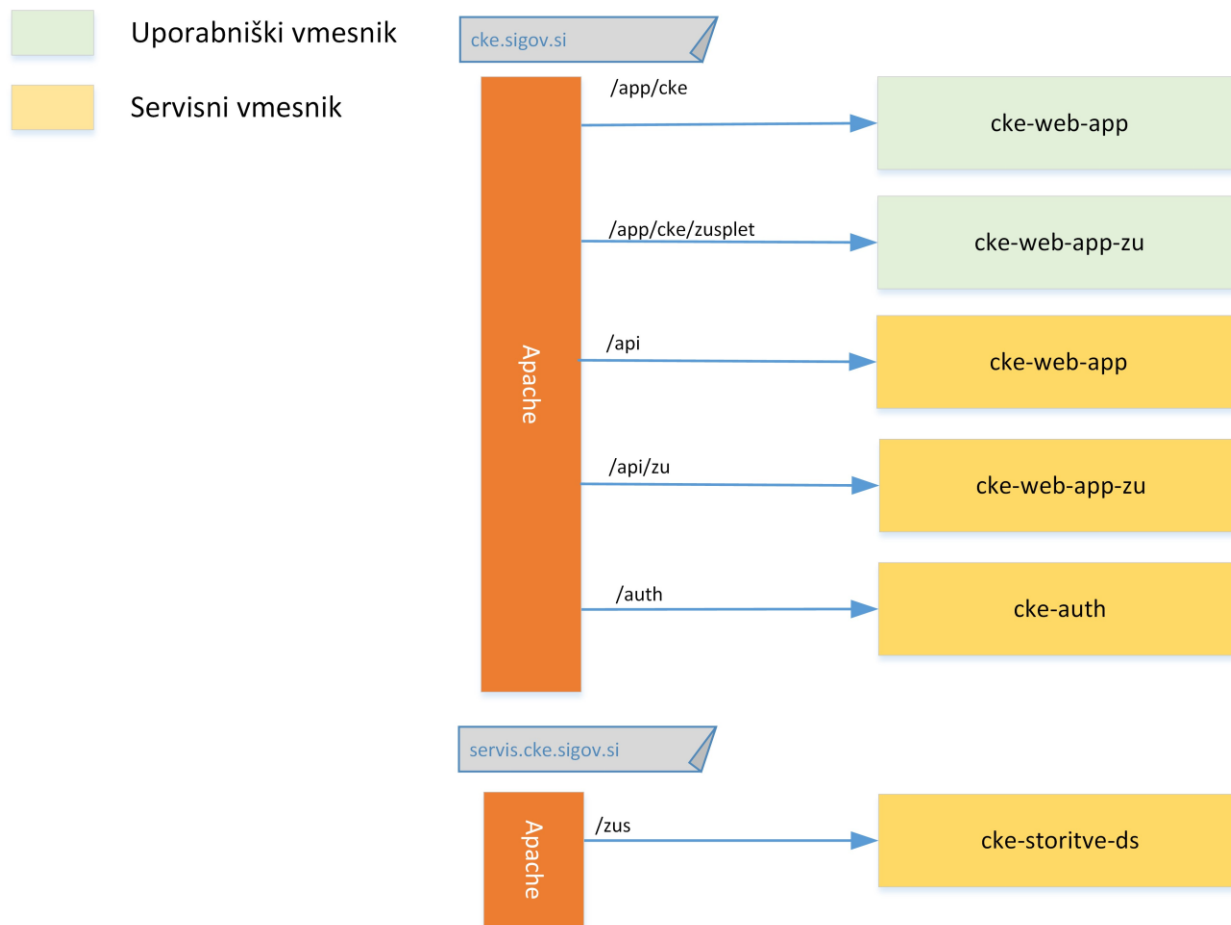
- **/auth**: avtorizacijski podsistem,
- **/app/cke**: vstopna točka za aplikacijo cke-web-app, ki nudi uporabniški vmesnik MP uporabnikom,
- **/app/cke/zusplet**: vstopna točka za aplikacijo cke-web-app-zu, ki nudi uporabniški vmesnik zunanjim uporabnikom,
- **/api**: vstopna točka za storitve aplikacije cke-web-app, ki nudijo podporo uporabniškemu vmesniku.

Spletno mesto servis.cke.sigov.si

- **/zus:** vmesnik do storitve zuServis (zus.asmx),

Za testno okolje sistema IS CKE se analogno uporabljata naslova:

- cke.pdc-test.sigov.si - naslov, kjer je dosegljiv testno okolje IS CKE,
- servis.cke.pdc-test.sigov.si - naslov, kjer je dosegljiv testni zuServis



Slika 2: Shema končnih točk

2.3.3 Podatkovna baza

Paketi, ki se nameščajo na podatkovno bazo, vključujejo tako skripte za vzpostavitev/nadgradnjo podatkovnih objektov kot tudi PL/SQL kodo, namenjeno izvajanju na podatkovni bazi v obliki paketov (packages).

Pri tem ločimo Oracle uporabnike (scheme), ki so lastniki podatkovnih objektov, ter uporabnike s katerimi posamezni moduli sistema dostopajo do podatkovne baze. Za modeliranje podatkov je uporabljen klasični entitetno relacijski pristop.

Za potrebe upravljanja in hrambe dokumentarnega gradiva je v uporabi dokumentni sistema Krpan.

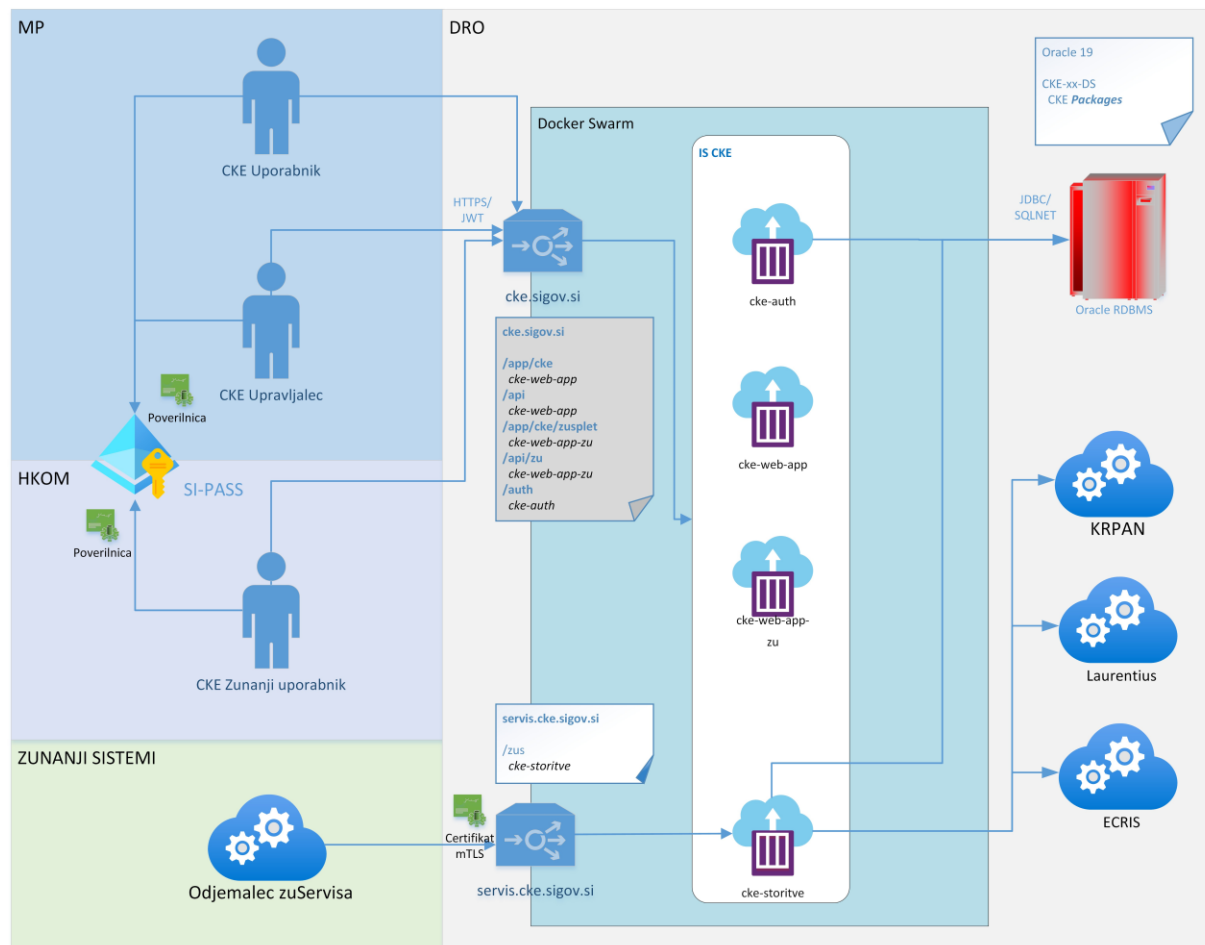


Izvedena je integracija, kar pomeni, da se aktivnosti povezane z ZUP ter ZVDAGA izvajajo znotraj sistema Krpan.

2.4 INFRASTRUKTURNI POGLED

2.4.1 Topologija sistema

Sistem je nameščen na DRO. Okvirno topologijo sistema prikazuje spodnja slika.



Slika 3: Predlog postavitve infrastrukture IS CKE



2.4.2 Mrežne povezave

Skladno s predlogom topologije so potrebne sledeče mrežne povezave:

Izvor			Cilj			Komunikacija	
Hostname	Modul	Cona	Hostname	Modul	Cona	Vrata	Protokol
Uporabnik	Brskalnik	HKOM	cke.sigov.si	Apache	LAN	443	https (TLS 1.2+)
cke.sigov.si	Apache	LAN	VLAN	cke-web-app	VLAN	80	http
CKE servisni odjemalec		HKOM	servis.cke.sigov.si	Apache	LAN	443	https (TLS 1.2+)
servis.cke.sigov.si	Apache	LAN	VLAN	cke-storitve	VLAN	80	http
IS CKE	cke-storitve	LAN	cke-db.sigov.si	Oracle	LAN	1521	SQLNET
IS CKE	cke-auth	LAN	cke-db.sigov.si	Oracle	LAN	1521	SQLNET



2.4.3 Nameščanje sistema

Nameščanje aplikacij sistema IS CKE izvaja upravljalec infrastrukture. Izvajalec v SVN odložišče naročnika na ustrezna mesta odloži:

- izvorno kodo javanskih paketov,
- izvorno kodo Angular paketov,
- izvorno kodo .Net Core paketov,
- dockerfile za izgradnjo Docker vsebnikov,
- pripadajoče bazne skripte, ki inkrementalno prilagodijo na ustrezno verzijo baznih objektov,
- spremljajoče dokumente (navodila za izgradnjo in namestitve),
- vsi drugi elementi, ki so potrebni, da naročnik samostojno prevede in izgradi aplikacijo v na ciljno okolje v namestljivi obliki.

Vsa predana javanska in .net core koda se lahko v celoti vključi v procedure avtomatskega prevajanja v izvršljivo obliko in grajenja namestitvenih paketov z vsemi odvisnostmi na okolju, vzpostavljenem na infrastrukturi MJU. Pri tem se uporabi orodje Maven oziroma .NET Core CLI. Javanska tehnologija je uporabljena pri izvedbo modula cke-auth.

3. NAVEZAVA NA ZUNANJE SISTEME

3.1 LAURENTIUS (VSRs)

Navezava na sistem Laurentius je namenjena digitalizaciji postopka prenosa kazenskih listov iz sodišča v CKE za obsodbe (kazenski listi), ki jih pošiljajo sodišča. Dokumenti se bodo prevzeli neposredno v čakalno vrsto CKE. Pri tem se uporabi že obstoječo lokalno instanco Laurentius-a na lokaciji MP, ki je povezana z VSRs.

Navezava na sistem Laurentius je enosmerna, kar pomeni, da je iniciator povezave vedno modul cke-storitve.

3.2 ECRIS

ECRIS (European Criminal Records Information System, European Criminal Records Information System - Third Country Nationals) Evropski informacijski sistem kazenskih evidenc ter ECRIS – TCN (European Criminal Records Information System - Third Country Nationals) Evropski informacijski sistem kazenskih evidenc – državljani tretjih držav sta sistema informacijskih povezav, ki uporabljata informacijsko tehnologijo za izmenjavo podatkov in informacij iz samostojnih kazenskih evidenc vsake države članice. Podatke se v njih izmenjuje z uporabo spletnih storitev (tehnologija SOAP), v zapisu XML.

V sistemu ECRIS in ECRIS - TCN poteka elektronska izmenjava podatkov in informacij iz kazenske evidence Republike Slovenije in kazenskih evidenc drugih držav članic, z uporabo enotnih standardiziranih oznak (šifre kaznivih dejanj, kazenskih sankcij, varnostnih ukrepov, držav, idr.). Sistema ECRIS in ECRIS – TCN bosta neposredno integrirana v IS CKE tako, da bodo sporočila drugih držav članic EU, prejeta preko sistemov, prihajala v aplikacijo kot vhodni dokumenti, odgovori na ta sporočila oziroma lastna sporočila MP pa bodo zapuščala aplikacijo kot izhodni dokumenti in bodo naprej posredovana naslovni državi članici oziroma sistemu ECRIS in ECRIS TCN. Poleg tega se bodo obsodilne sodbe zoper državljane DČ EU oziroma tretjih držav in oseb brez državljanstva poslale v



sistema.

Navezava na sistem ECRIS je enosmerna, kar pomeni, da je iniciator povezave vedno modul cke-storitve.

3.3 ZUSERVIS - SPLETNI SERVIS SISTEMA IS CKE

Zunanji odjemalci se navezujejo na IS CKE z uporabo SOAP servisa zuServis.

Pooblaščenca zunanja institucija tako pokliče ta servis, za vrste dokumentov, ki so podlaga za vpis (prenos) podatkov v CKE in sicer:

- Zahtevek,
- Obvestilo o izvrševanju kazenske sankcije.

Pošiljke pridejo v IS CKE v obliki XML zahtevka. Sistem periodično (na nekaj minut) zajema prejete XML-je ter jih pretvori v sporočila na način, ki je podrobno opisan v dokumentu »IS CKE Funkcionalne specifikacije v 4.0.pdf«, v poglavju 6.2.1, točka 2.

3.4 CRP (MNZ)

Navezava na CRP je izveden z dostopom do ti. distribucijske kopije CRP (IO-CRP), ki jo MNZ vzdržuje na distribucijski komponenti IO-Modul2 na infrastrukturi MJU. Gre za isto kopijo CRP, kot jo za svoje potrebe uporabljajo platforma e-Sociala oz. še številni drugi javni organi. Do nje se dostopa neposredno z uporabo klica storitve.

3.5 PRS (AJ PES)

IS CKE uporablja spletno (SOAP) storitev wsPrsInfo, katere lastnik storitve je AJ PES.

4. VARNOST

4.1 UPORABNIKI SISTEMA

Vsi uporabniki sistema IS CKE se avtentikirajo z uporabo horizontalne komponente SI-CAS. Avtentikacija je omogočena z visokim nivojem prijave oz. katerikoli načinom prijave, ki ga omogoča gradnik SI-CAS in bo dogovorjen z naročnikom.

V sistemu IS CKE z varnostnega pogleda ločimo naslednje segmente uporabnikov:

- zunanji uporabniki IS CKE,
- notranji uporabniki IS CKE,
- uporabniki s posebnimi pooblastili.

4.2 UPRAVLJANJE Z IDENTITETAMI IN DOSTOPI UPORABNIKA

Sistem IS CKE vsebuje gradnik **cke-auth** (v nadaljevanju auth modul), ki deluje kot posrednik do centralnih gradnikov SI-CAS in Centralna Varnostna shema.

Varnostna shema je horizontalni gradnik, čigar uporaba je predpisana v razpisni dokumentaciji in pokriva



zahtevane funkcionalnosti iz točke 9.2.16.1.1. Opis varnostne sheme je definiran v dokumentaciji, ki je dostopna na povezavi <https://vs.gov.si/VS.web/>.

4.2.1 Identifikacija uporabnikov z uporabo gradnika SI-CAS

Za identifikacijo uporabnikov se uporabi centralni avtentikacijski sistem SI-CAS. Na centralnem avtentikacijskem sistemu SI-CAS se lahko uporabnik predstavi na različne načine.

Za uporabo IS CKE je zahtevan nivo prijave, ki zagotavlja visoko stopnjo zaupanja.

Identifikacija uporabnika je izvedena s pomočjo povezovalnega modula auth, ki za potrebe same avtentikacije uporabi gradnik SI-CAS. Sistem SI-CAS po uspešni avtentikaciji posreduje IS CKE sistemu sledeče podatke:

- uporabljen nivo prijave,
- uporabljen instrument prijave,
- podatki o uporabniku,
- avtorizacijske podatke iz CVS.

4.2.2 Avtorizacija uporabnikov

Avtorizacija oz. pravice uporabnikov sistema temelji na vlogah. Vloga je definirana kot skupina funkcionalnosti in omejitev pri uporabi funkcionalnosti sistema. Vsakemu uporabniku je predpisana vsaj ena ali več vlog, ki izhajajo iz organizacijskega profila oz. segmenta uporabnika. Vloge uporabnika se hranijo v gradniku CVS, kjer se tudi upravljajo.

Vsak uporabnik sistema IS CKE ima lahko enega ali več uporabniških profilov, ki so tipično vezani na določeno organizacijo. Profil vsebuje tudi podatke o delovnem mestu in njegovi umestitvi v organizacijo.

4.2.3 Avtentikacija in avtorizacija odjemalcev zuServis-a

Servisni uporabniki sistema IS CKE dostopajo do sistema izključno preko storitve zuServis.

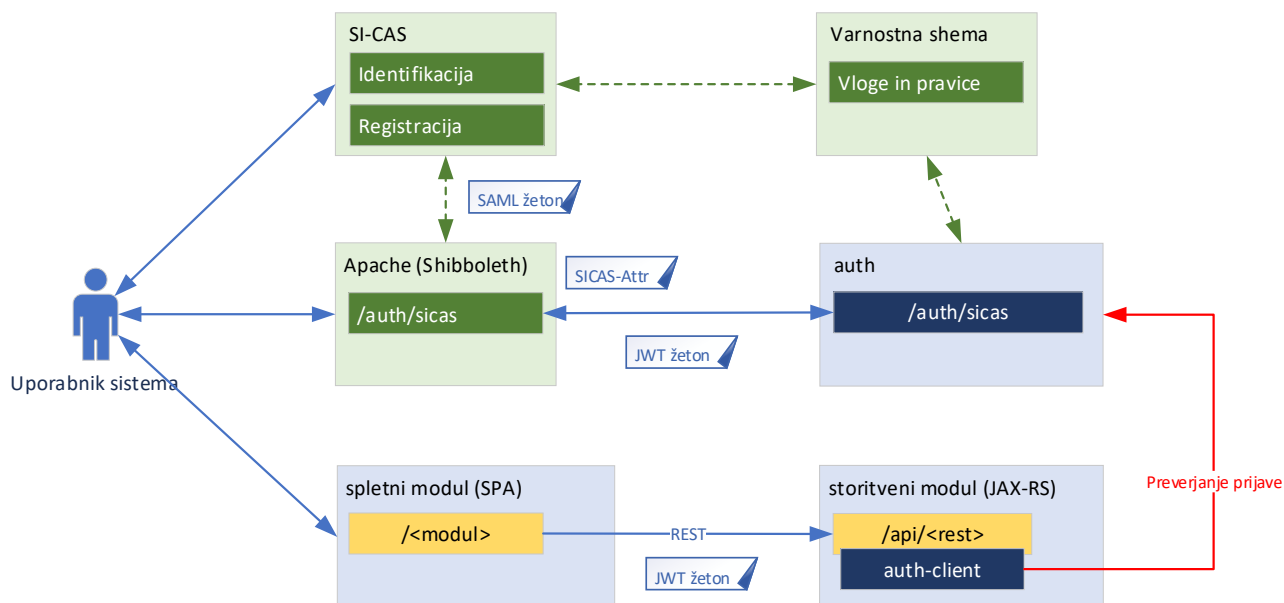
Na vstopni točki servisa je zahtevana identifikacija odjemalca s pomočjo mTLS. Odjemalec ob klicu tako posreduje x509 digitalno potrdilo s katerim se identificira. V nadaljnjem koraku se v IS CKE sistemu preveri identiteta odjemalca in njegove pravice. Na osnovi dobljenega se odjemalcu omogoči izvedbo do IS CKE storitve.

4.2.4 Gradniki infrastrukture

Infrastrukturo sestavljajo:

- **SI-CAS:** horizontalni gradnik namenjen identifikaciji uporabnika IS CKE. Sistem sestavljata zunanji sistem, kjer se identifikacija dejansko izvede (<https://sicas.gov.si>) ter razširitveni modul za Apache (mod_shib), ki je nameščen na spletnem strežniku sistema.
- **CVS:** horizontalni gradnik namenjen upravljanju avtorizacijskih podatkov uporabnika. Na gradniku se urejajo vloge, pravice glede na organizacijsko strukturo. Gradnik zagotavlja tudi končno avtorizacijsko točno sistemskih uporabnikov.
- **cke-auth:** povezovalni modul, ki zagotavlja povezovanje v enotno avtentikacijsko in avtorizacijsko točko za sistem
- **cke-auth-client:** namenska knjižnica, ki jo uporabljajo vsi povezani elementi sistema IS CKE z

modulom auth in poskrbi za pravilno upravljanje z avtentikacijskimi in avtorizacijskimi podatki uporabnika.



Slika 4: Gradniki varnostne infrastrukture SI-CAS

4.2.5 Delovanje

Scenarij uporabe SI-CAS varnostnega sistema je sledeč:

Uporabnik spletnega mesta z uporabo brskalnika zahteva zaščiten vsebino (1). Ker uporabnik še nima ustreznega piškotka z žetonom JWT, se pošlje brskalniku (2) redirect (302) na lokacijo /auth/sicas.

Lokacija /auth/sicas (3) je na spletnem strežniku pod nadzorom Shibboleth Apache razširitvenega modula, ki preveri, če je v zahtevku piškotek tega modula. Če ga ni, se preveri ali je v glavi zahtevka SAML žeton iz SI-CAS-a. Če ga ni, se ga preusmeri na SI-CAS spletno mesto (4) (302).

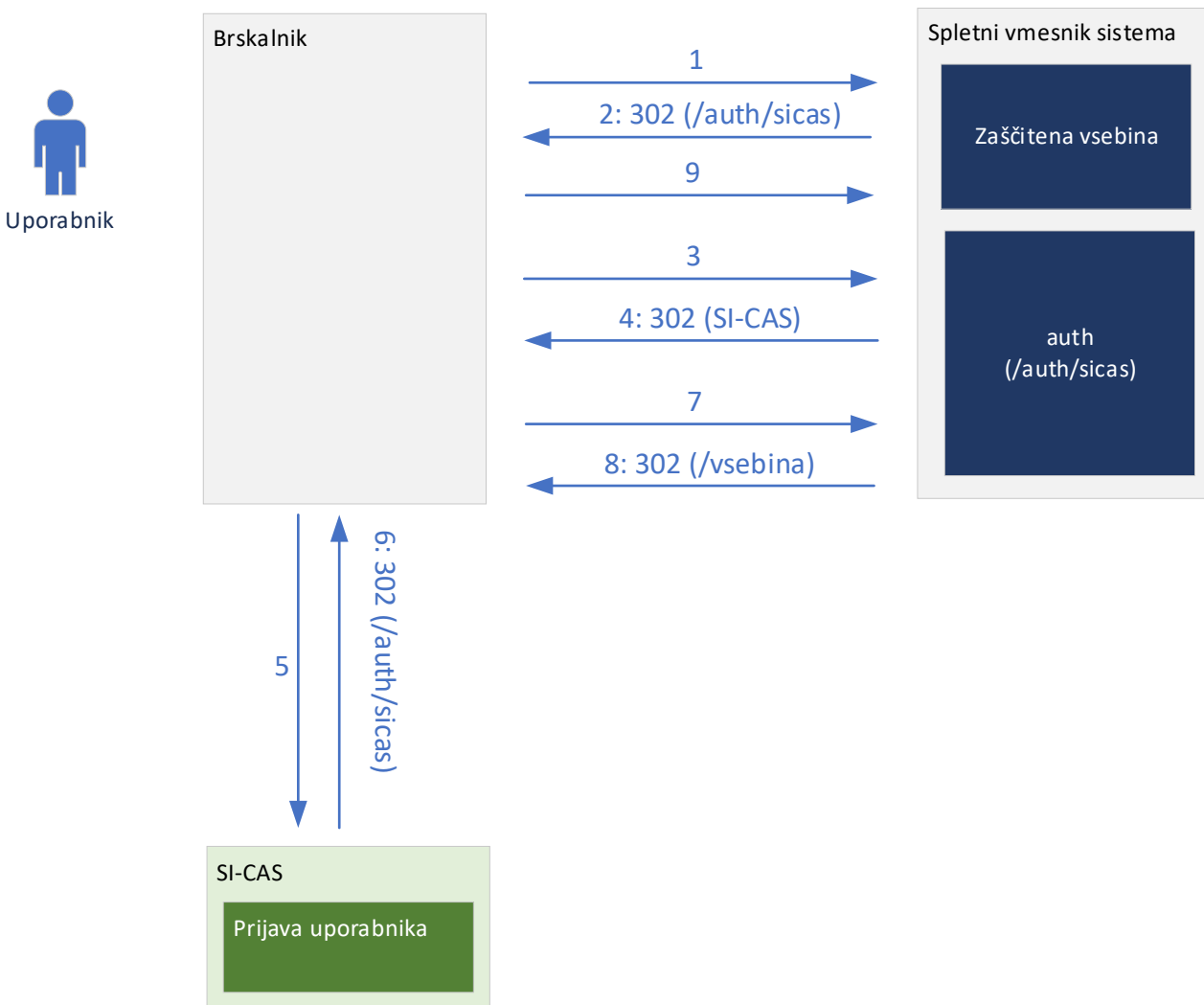
Na SI-CAS spletnem mestu (5) se uporabnik identificira z izbranim avtentikacijskim mehanizmom. Po uspešni identifikaciji se uporabnika preusmeri nazaj na lokacijo /auth/sicas (6).

V tem primeru Shibboleth modul nastavi v glavo zahtevka izbrane SI-CAS attribute in spusti klic do ciljnega spletnega naslova /auth/sicas na povezovalnem modulu auth.

Povezovalni modul auth iz glave zahtevka pobere SI-CAS attribute in jih shrani (7). V nadaljevanju se kreira JWT žeton in se ga kot piškotek na / kontekstu vrne uporabniku (brskalniku) hkrati s preusmeritvijo na izvirno zahtevo na vsebino spletne aplikacije (8).

Ko zahtevek ponovno pride do spletne aplikacije (9), vsebuje piškotek z žetonom JWT. Aplikacija s pomočjo modula auth preveri ali je žeton veljaven (preverjanje podpisa). Poleg same validacije žetona se lahko hkrati tudi na auth pridobi osnovne informacije o uporabniku ter njegovih pravicah.

JWT žetoni se prav tako uporabijo pri komunikacij med internimi klici REST storitev. Tehnično se uporabljajo trije piškotki SI-CAS, apache-shibboleth ter auth, ki je tipa »http only« in »secure«.



Slika 5: Prijava uporabnika IS CKE

Modul v podatkovni bazi shranjuje podatke o sejah uporabnika ter attribute uporabnika, ki jih v postopku prijave pridobi od sistema SICAS (odvisno od načina prijave na SICAS ter stopnje zaupanja). Do podatkov se dostopa izključno z uporabo shranjenih postopkov pri tem pa uporablja dva različna aplikacijska bazna uporabnika. Prvega uporablja API vmesnik, ki se uporablja pri prijavi in drugega administrativni vmesnik modula, vsak pa ima minimalni nabor pravic. API vmesnika sta ločena, tako, da se lahko tudi na mrežnem nivoju omeji dostopnost vmesnikov.

Lahko se uporabi več instanc modula tudi v različnih mrežnih segmentih, vendar naj moduli uporabijo skupno podatkovno bazo.

4.3 KONTROLA PRISTOPA

Kontrolo pristopa do sistema se izvaja na več spodaj opisanih nivojih.



4.3.1 Kontrola pristopa na nivoju uporabniškega vmesnika

Za kontrolo pristopa na uporabniškem vmesniku se uporablja kontrola pristopa, ki je vgrajena v modulu auth. Pri tem je potrebno poudariti, da se sama identifikacija uporabnika izvede na zunanjem sistemu SI-CAS. Vgrajeni sistem kontrole pristopa se uporabi za:

- identifikacijo uporabnika; zanesljivo in varno se ugotovi identiteta uporabnika in se mu omogoči uporaba sistema na varen način;
- avtorizacija uporabnika; zagotovi se, da ima uporabnik ustrezne pravice za izvedbo določene aktivnosti.

4.3.2 Kontrola dostopa na nivoju podatkovne baze

IS CKE uporablja namensko postavljenega baznega uporabnika za dostop do podatkovnih objektov. Ta uporabnik ni lastnik shem in ima dodeljene le pravice do izvajanja tistih namensko spisanih baznih procedur/funkcij/viewev, ki jih za svoje delovanje nujno potrebuje.

4.4 VAROVANJE OMREŽNEGA PROMETA

Komunikacijo med zunanjim uporabnikom in spletnim strežnikom se varuje preko protokola TLS, ki je IETF standard track protokol, nazadnje osvežen v RFC 5246. Uporablja se TLS verzije 1.3. Z navedenim transportom zagotavljamo strežniško identifikacijo uporabniku in s tem preprečujemo uporabo lažnih spletnih naslovov. Vsa komunikacija med sistemom IS CKE in zunanjimi sistemi, kot tudi med posameznimi moduli sistema IS CKE, če se ti nahajajo v različnih omrežnih segmentih je šifrirana.

5. NADZOR IN UPRAVLJANJE SISTEMA

V poglavju so opisani mehanizmi in postopki za nadzor in upravljanje sistema v realnem času, tako s stališča:

- administracije sistema,
- spremljanja delovanja sistema in
- revizijske sledi.

5.1 UPRAVLJANJE SISTEMA

V sklopu nadzora se lahko s pomočjo funkcionalnosti aplikacije cke-app pregleduje in ureja poslovne nastavitve sistema IS CKE (npr. urejanje šifrantov). Znotraj aplikacije se lahko spreminja določene poslovne parametre sistema, kot tudi spremlja samo delovanje sistema.

Za uporabo aplikacije so potrebne ustrezne poverilnice in pravice. Sama uporaba modula je omejena na MP.

Sistemske nastavitve sistema IS CKE (kot so proxy, URL, lokacija truststora, certifikatov ...) se nahajajo v zunanjih konfiguracijskih datotekah, ki se ne prepisujejo z deployem spletnega servisa/modula in je specifična okolju, na katerem teče sistem.

5.2 SPREMLJANJE DELOVANJA SISTEMA

Dnevniški zapisi



Rešitev IS CKE za logiranje uporablja funkcionalnost ogrodja Quarkus (<https://quarkus.io/guides/logging>) oz. .Net Core (Microsoft.Extensions.Logging). Tako se glede na konfiguracijo lahko vodi datotečni dnevnik za katerega je možno nastaviti nivo logiranja običajno preko nastavitvene datoteke oz. zagonskih parametrov.

Datoteke so dostopne na datotečnem sistemu, pregledovanje pa je urejeno v centralnem pregledovalniku dnevniških datotek DRO okolja na naslovu: <https://monitor.sigov.si/appllog2>

5.3 REVIZIJSKA SLED SISTEMA

Revizijska sled se uporablja za nadzor in preverjanje dostopa do osebnih podatkov. Sistem zagotavlja beleženje revizijske sledi za vse aktivnosti povezane uporabo aplikacij IS CKE, kot tudi vse dostope do zunanjih spletnih storitev.

Zagotovljeno je, da se v revizijsko sled zapiše:

- kdaj je,
- kdo dostopal,
- do česa (kaj) in,
- s kakšnim namenom.

Prav tako se ob klicu zunanjih sistemov zabeleži eventualna povratna informacija kot npr. id transakcije in podobno z namenom zagotavljanja celotne povezane revizijske sledi.

Pregled revizijske sledi se izvaja z uporabo uporabniškega vmesnika znotraj IS CKE, ki je namenjen notranjim uporabnikom.

Revizijska sled v podatkovnem izvajalnem okolju Oracle DB

Na podatkovnem nivoju je revizijska sled realizirana s standardnimi audit tabelami.

Sledljivost obdelave osebnih podatkov je opisana tudi v dokumentu »IS CKE Funkcionalne specifikacije v 4.0.pdf«, v poglavju 13.

6. OKOLJA

Za IS CKE sta vzpostavljeni dve ločeni okolji, ki bosta nameščeni na MJU infrastrukturi in dve okolji, nameščeni pri izvajalcu SRC:

- Izvajalec (SRC):
 - razvojno okolje (RDN),
 - testno okolje (TSN).
- Lastnik in upravljevec centralne infrastrukture (MJU – 3 GEN):
 - testno okolje (TEST),
 - produkcijsko okolje (PROD).



6.1 OKOLJA PRI LASTNIKU IN UPRAVLJALCU CENTRALNE INFRASTRUKTURE (MJU)

OKOLJE	TEST	PROD
Namen	<ul style="list-style-type: none"> - Testiranje vseh funkcionalnosti sistema. - Testiranje novih verzij rešitve. - Testiranje povezovanja z zunanjimi testnimi sistemi 	<ul style="list-style-type: none"> - Producersko delovanje sistema. - Povezava na vse zunanje sisteme.
Podatki	Testni podatki	Producerski podatki
Občutljivost podatkov	NE	DA
Povezovanje z zunanjimi sistemi	DA (testni zunanji sistemi)	DA (producerski zunanji sistemi)
Uporabniki	<ul style="list-style-type: none"> - Testni uporabniki sistema - Zunanji testni informacijski sistemi 	<ul style="list-style-type: none"> - Uporabniki producerskega sistema - Zunanji producerski informacijski sistemi
Lokacija	MJU	MJU

Slika 6: Okolja lastnika in upravljalca centralne infrastrukture (MJU)

6.2 OKOLJA IZVAJALCA (SRC)

OKOLJE	Razvojno	Testno
Namen	<ul style="list-style-type: none"> - Razvoj funkcionalnosti sistema - Razvoj novih verzij rešitve 	Interno testiranje razvitih funkcionalnosti sistema.
Podatki	Razvojni podatki	Testni podatki, pripravljeni s strani izvajalca
Občutljivost podatkov	NE	NE

Povezovanje z zunanjimi sistemi	NE	DA (razvojno/testna okolja zunanjih sistemov)
Uporabniki	Razvojni inženirji	Testerji izvajalca
Lokacija	SRC	SRC

Slika 7: Okolja izvajalcev

7. UPORABLJENI STANDARDI IN TEHNOLOGIJE

V okviru IS CKE so predvideni naslednji odprti standardi in tehnologije:

- **REST** (http://en.wikipedia.org/wiki/Representational_state_transfer) – REST je protokol za izmenjavo strukturiranih informacij preko spletnih servisov običajno z uporabo JSON objektov.
- **JSON** (<http://www.json.org/>) - tip notacije, zaradi svoje strnjivosti, primeren za serializacijo in komunikacijo med odjemalcem in strežnikom kot tudi strežniškimi sistemi.
- **XML** (<http://en.wikipedia.org/wiki/XML>) – označevalni jezik, ki definira pravila za opis strukturiranih podatkov, primeren za serializacijo in komunikacijo med odjemalcem in strežnikom kot tudi med strežniškimi sistemi.
- **JavaScript** (<http://en.wikipedia.org/wiki/JavaScript>) - objektni skriptni programski jezik za ustvarjanje spletnih interaktivnih strani. Podpirajo ga vsi novejši spletni brskalniki.
- **TypeScript** (<https://en.wikipedia.org/wiki/TypeScript>) – objektno orientiran odprtokodni programski jezik uporaben za izdelavo JavaScript aplikacij.
- **CSS3** (http://en.wikipedia.org/wiki/Cascading_Style_Sheets) - standard (jezik) za prikaz grafičnih efektov in oblik na spletnih straneh. Podpirajo ga vsi novejši spletni brskalniki.
- **HTML5** (<http://en.wikipedia.org/wiki/HTML5>) - standard (jezik) za izdelavo spletnih strani. Podpirajo ga vsi novejši spletni brskalniki.
- **Apache Web Server** (<http://httpd.apache.org>) - najbolj razširjeni odprtokodni spletni strežnik. Podpira zelo raznolike storitve (proxy, SSL, navidezni host-I, podpora jezikom – PHP, Perl, Python...).
- **Docker** (<http://docker.com>) – tehnologija vsebnikov, ki olajša upravljanje sistema in hkrati omogoča boljši izkoristek sistemskih virov.
- **Java SE11**
- **Java EE8** - standard za Java enterprise spletne aplikacije, ki med drugim vključuje naslednje standarde, ki se lahko uporabijo v okviru sistema IS CKE:
 - **Java API for RESTful Web Services (JAX-RS)** – standardni javanski API za izdelavo spletnih storitev po principu REST.
 - **Java API for XML-Based Web Services (JAX-WS)** - standardni javanski API za izdelavo spletnih storitev (web services).
 - **Java Architecture for XML Binding (JAXB)** – standardni javanski API za serializacijo in deserializacijo javanskih objektov v/iz XML zapisa.
- **.NET CORE** – prosti odprtokodni sistem, naslednik ogrodja .NET, ki podpira različne platforme
- **JDBC** (http://en.wikipedia.org/wiki/Java_Database_Connectivity) - javanski vmesnik za dostop do relacijskih podatkovnih baz npr. Oracle, MySQL, ipd.
- **JPA** (https://en.wikipedia.org/wiki/Java_Persistence_API) – javanski programski vmesnik za opis in upravljanje relacijskih podatkov.
- **Eclipse Microprofile** – platforma za izdelavo mikrostoritev, ki vključuje tudi Health in Metrics



specifikacije in temelji na Java EE.

- **Apache CXF** (<http://cxf.apache.org/>) – odprtokodno ogrodje, ki nam omogoča izdelavo storitev za različne protokole (REST, SOAP, XML/HTTP...)
- **JBoss RestEasy** (<https://resteasy.github.io/>) – odprtokodno ogrodje za izdelavo REST storitev
- **Apache Maven** (<http://maven.apache.org/>) – odprtokodno orodje, ki nam olajša in avtomatizira delo s projekti (build, deploy, test ...)
- **Quarkus** (<https://quarkus.io/>) – ogrodje za izdelavo mikrostoritev
- **Apache Commons** (<http://commons.apache.org/>) – skupek odprtokodnih knjižnic, ki olajšajo delo s standardnimi javanskimi razredi.
- **JUnit** – javansko ogrodje za podpora unit testom (<http://junit.org/>)
- **Quartz** (<http://quartz-scheduler.org/>) - javanska odprtokodna knjižnica, ki nam omogoča časovno zaganjanje storitev (scheduling) v javanskih aplikacijah.
- **JasperReports** – javansko ogrodje za izdelavo poročil (<http://community.jaspersoft.com/project/jasperreports-library>)
- **xdocreport** - Javanska knjižnica za podpora dokumentnim formatom (<https://github.com/opensagres/xdocreport>)
- **Angular** (<https://angular.io/>) – odprtokodno JavaScript ogrodje za izdelavo predstavitvenega dela modernih spletnih aplikacij.

7.1 STANDARDI IN TEHNOLOGIJE ORACLE PODATKOVNE BAZE

V okviru IS CKE se bodo uporabljali naslednji Oracle standardi in tehnologije:

- **DataGuard** - Mehanizem za prenos sprememb na bazi na alternativno lokacijo - uporablja ga upravljalca MJU infrastrukture.
- **Stored procedure** - logično zaključene celote programske kode, ki se izvedejo na baznem nivoju.
- **Database Views** – Podatkovni pogledi na podlagi shranjenih poizvedb.