



IS Monitoring - Tehnološka zasnova

Verzija 0.90



Številka dokumenta:	218509	Verzija:	0.90
Projekt:	ARSO-MON	Datum:	07.05.2026
Skrbnik:	Gašper Štepec	Odobril:	Marko Račeta

Zgodovina

Datum	Verzija	Oseba	Opis
06.11.2023	0.10	Nataša Naglič, Marko Račeta, Jože Mlakar	Prva verzija dokumenta
22.11.2023	0.20	Nataša Naglič, Marko Račeta, Jože Mlakar	Dopolnitve glede na naročnikove komentarje.
15.01.2024	0.30	Nataša Naglič, Marko Račeta, Jože Mlakar	Dopolnjene slike, poglavje 3.
24.01.2024	0.40	Nataša Naglič, Marko Račeta, Jože Mlakar	Dodano pojsnilo glede uporabe tehnologije Websocket.
13.11.2024	0.50	Marko Račeta, Gašper Štepec, Rok Švikart	Dopolnjeno poglavje Upravljanje z uporabniki. Posredovano naročniku 15.11.2024
03.12.2024	0.60	Marko Račeta, Gašper Štepec, Rok Švikart	Dopolnjeno poglavje Upravljanje z uporabniki. Popravljene vnosne maske. Posredovano naročniku 3.12.2024.
04.12.2024	0.70	Marko Račeta, Gašper Štepec, Rok Švikart	Dopolnjeno poglavje Upravljanje z uporabniki. Popravljene vnosne maske. Posredovano naročniku 4.12.2024.
08.07.2024	0.80	Marko Račeta, Gašper Štepec, Rok Švikart	Dodano poglavje Integracija z IS Dovoljenja. Posredovano naročniku 8.7.2025
07.05.2026	0.90	Marko Račeta, Gašper Štepec, Rok Švikart	Čistopis dokumenta.

Kazalo

1.	Uvod.....	56
2.	Popis uporabljenih tehnologij	56
2.1.	Predstavitveni nivo	67
2.2.	Poslovna logika	78
2.3.	Kontejnerji	94
2.4.	Podatkovni nivo	94
2.5.	Dokumentni nivo	104



3.	Neprekinjena integracija in neprekinjena dostava/neprekinjeno uvajanje	1041
3.1.	Mape izvorne kode	1142
3.2.	Mape namestitvenih objektov	1243
4.	Arhitektura sistema za implementacijo	1243
5.	Varnostni in zaščitni mehanizmi	1314
5.1.	Arhitekturni nivo	1314
5.2.	Zaščita komunikacijskih kanalov.....	1314
5.3.	Sistemi nivo	1415
5.4.	Omejevanje dostopa	1415
5.5.	Zaščita pred tretjimi osebami.....	1516
5.6.	Avtentikacija uporabnikov	1718
5.7.	Avtentikacija zunanjih sistemov	1920
5.8.	Podatkovni nivo	1920
6.	Integracije z zunanjimi sistemi.....	1920
6.1.	Integracije preko podatkovne zbirke	1920
6.1.1.	Podatki so izvirno v IS Monitoring	2021
6.1.2.	Podatki so izvirno izven IS Monitoring	2021
6.2.	Integracije z uporabo API	2021
6.2.1.	Iniciator klicev	2021
6.2.2.	Integracije, kjer ima IS Monitoring vlogo klicatelja	2122
6.2.3.	Integracije, kjer ima IS Monitoring vlogo čakajočega na klic	2122
6.2.4.	Integracija z IS Dovoljenja	2122
7.	Upravljanje z uporabniki	2223
7.1.	Tehnični administratorji IS Monitoring SSO	2223
7.2.	Registracija novih uporabnikov aplikacij IS Monitoring	2223
7.2.1.	Registracija z uporabo zunanje storitve SI-CAS	2223
7.2.2.	Registracija z ročno registracijo zunanje storitve	2425
7.2.3.	Registracija z ročno registracijo uporabnika, ki uporablja uporabniško ime in geslo	2425
7.3.	Zahtevek za dodelitev in/ali odvzem dostopa	2526
7.3.1.	Oddaja zahtevka za dodelitev in/ali odvzem dostopa	2526
7.3.2.	Pooblaščenje na nivoju kompleksov	2728
7.4.	Krovne vloge	2728
7.5.	Profili (Organizacije) uporabnikov	2728
7.6.	Administracija uporabnikov	2829
7.6.1.	Stran seznam uporabnikov	2829
7.6.2.	Stran Uporabnik	2930





1. Uvod

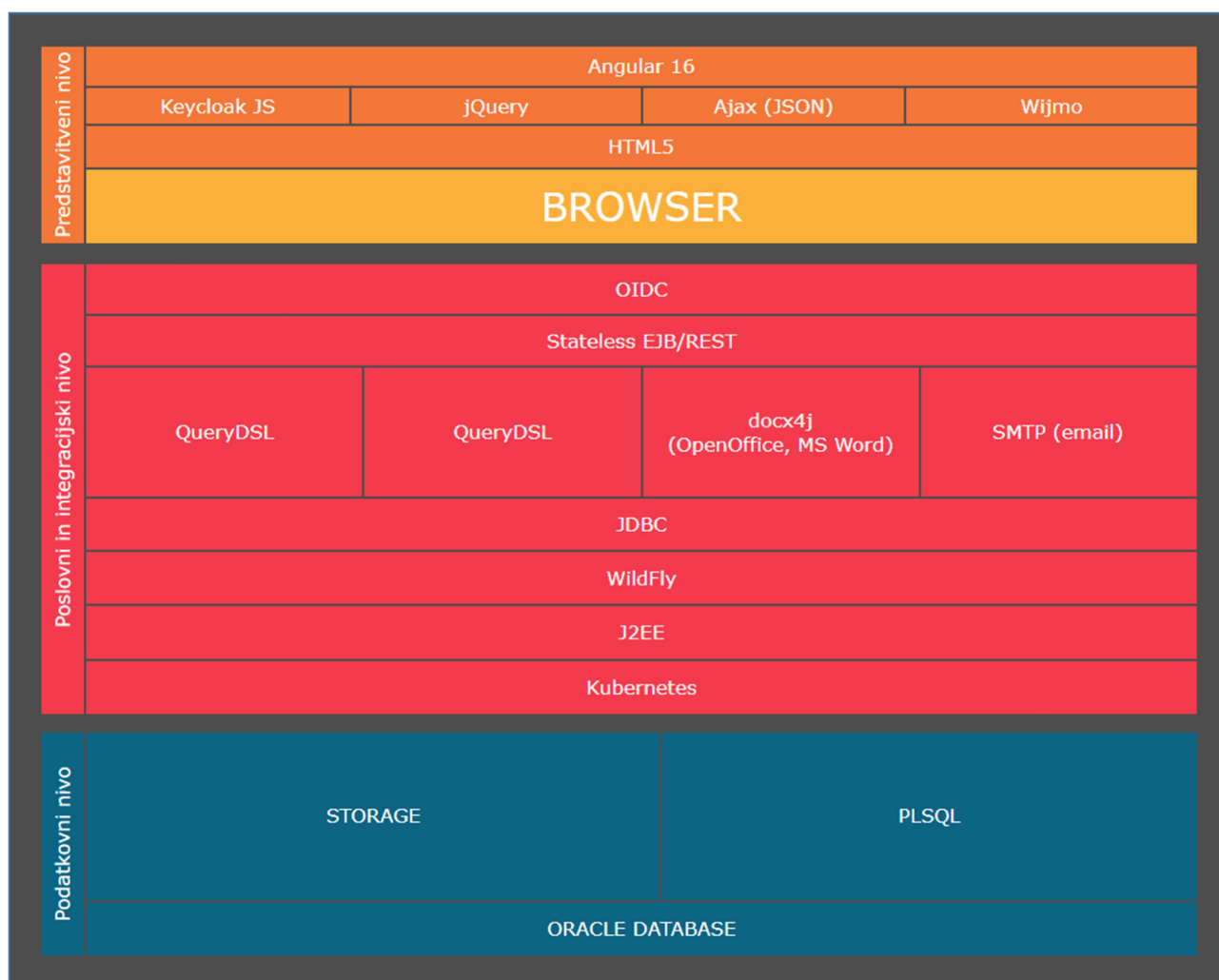
Agencija Republike Slovenije za okolje (ARSO) vzpostavlja nov IS za podporo procesom obratovalnih in državnih monitoringov.

V nadaljevanju dokumenta je opisana tehnološka zasnova sistema.

2. Popis uporabljenih tehnologij

V nadaljevanju je opis vseh tehnologij, ki bodo uporabljene znotraj sistema. IS Monitoring predvideva izključno atributno aplikacijo. GIS podsistem ni predmet tega projekta in se IS Monitoring dotika zgolj skozi posamezne tabele (na primer podatki slojev, ki se bodo uvozili v bazo in IS Monitoring bo nad njimi lahko izvajal operacije/poizvedbe za namen določitve MM), ki jih ARSO GIS prikaže.

Arhitekturno gre za spletne več-nivojske aplikacije brez gradnikov na strani odjemalca z izjemo brskalnika (podprti so vsi glavni brskalniki, brez posebnih vtičnikov).



Slika 1: Arhitektura komponent sistema po nivojih



2.1. Predstavitveni nivo

Uporabljena je tehnologija Angular 17, ki predstavlja preizkušeno rešitev posebej primerno za zahtevne informacijske sisteme. Gre za tehnologijo, ki v celoti sloni na delovanju brskalnika (HTML5). Deluje v celoti znotraj brskalnikov (podprti so najbolj popularni brskalniki zadnjih različic), zato je sistem bolj neodvisen od operacijskega sistema končnega uporabnika oziroma naprave in zahteva manj (nič) nastavitvev okolja uporabnika. Takšen sistem je mogoče v polni funkcionalnosti uporabiti tudi na sodobnih mobilnih napravah.

Aplikacija v domeni ARSO deluje kot aplikacija v brskalniku (single page application – SPA), kar predstavlja boljši izkoristek strežniške opreme, saj strežniška oprema aplikacijo posreduje uporabniku kot statično vsebino, podatke pa aplikacija pridobi preko REST protokola. Sporočila s **strežnika proti aplikaciji** (na primer o zaključeni obdelavi, novih podatkih in podobno) sistem posreduje z uporabo WebSocket (nadgradnja protokola http). Sporočila niso vrste zanesljive dostave (reliable messaging), zato ni potrebna namestitev strežniških sporočilnih vrst. Takšna zasnova skupaj z nalaganjem modulov na zahtevo (lazy load) omogoča uporabo kompleksne aplikacije tudi v brskalnikih, ki imajo močno omejene kapacitete (starejši računalniki). Kljub vsemu je treba poudariti, da zaradi zastarelih šifrirnih mehanizmov brskalnikov na **zastarelih operacijskih sistemih** (na primer Windows XP, Windows Vista), **ki jih proizvajalci ne posodablajo več, sistem na takšnih operacijskih sistemih ne bo deloval.**

Če se bo izkazalo, da zgoraj omenjena tehnologija WebSocket povzroča težave na omrežni opremi bomo skupaj z naročnikom našli ustreznejšo tehnologijo, na podlagi analize in opreme takrat. Takšno spremembo bomo izvedli v garancijski obliki (brez dodatnih stroškov za naročnika).

Podpora brskalnikom je objavljena na <https://angular.io/guide/browser-support> ki je deklarativne narave. Zaradi nenehnega razvoja je nemogoče "ujeti" deklarativno podporo za vse brskalnike, ki so v uporabi. V praksi pa s tem nismo zasledili težav. Izjema so stari brskalniki in nekatere specifične različice brskalnikov s konkretnimi napakami.

Več o varnostnih mehanizmi v poglavju 5 Varnostni in zaščitni mehanizmi, tu le povzetek: Avtentikacija temelji na protokolu OIDC. Aplikacija v domeni IS Monitoring ob zagonu preveri, ali ima uporabnik na voljo žeton za varovanje sistema. Praviloma takšnega žetona nima (razen, ko odpre nov listič v brskalniku), zato ga aplikacija preusmeri na centralni avtentikacijski sistem IS Monitoring, ki tako služi tudi kot SSO (single sign-on). Po zaključeni avtorizaciji (bodisi interno v IS Monitoring SSO ali po posredovanju na zunanjo storitev) IS Monitoring SSO uporabnikov brskalnik preusmeri nazaj na aplikacijo z uporabo globokih povezav (deep link) in z žetonom za varovanje sistema. Tako uporabnik lahko transparentno dostopa do konkretne vsebine v sistemu (in ne izključno do začetne strani). Aplikacija ob vsakem zahtevku do poslovnega nivoja poda žeton kot del zahtevka. Ker ima žeton izredno kratko veljavnost (5 minut), aplikacija pred vsakim dostopom preveri starost žetona in po potrebi (če je starejši od štirih minut) na IS Monitoring SSO izda zahtevek za osvežitev žetona (z uporabo REST klica). Tako uporabniku ni treba izvajati ponovne prijave vsakih 5 minut, sistem pa je varovan z vedno svežim žetonom. Zaradi časovne omejenosti trajanja žetona je pomembna časovna usklajenost (zahtevana je usklajenost do 1 min natančno) uporabnikovega sistema s centralnim sistemom. Uporabnika ob odstopanju ure o tem obvestimo.

Poslovni nivo in seje na podatkovni zbirki bosta v celoti izdelana kot stateless (poslovni nivo ne hrani stanja seje), kar olajša razširljivost sistema in bistveno zmanjša pomnilniški odtis uporabnika na strežniku.



Oblikovanje aplikacije temelji na responsive design, tako da se aktivno prilagaja napravi uporabnika.

Sistem za analitiko in IS Monitoring SSO so odprtokodne rešitve, katerih uporabniški vmesnik temelji na JSF tehnologiji.

Uporabljeni so standardi http, REST, HTML5, WebSocket, Angular 16, TypeScript, JSON, Javascript.

Specifikacije uporabljenih tehnologij:

<https://tools.ietf.org/html/rfc2068> http

<https://tools.ietf.org/html/rfc7231> http vsebina (REST)

<https://tools.ietf.org/html/rfc6455> WebSocket

<https://www.w3.org/TR/html5/> HTML5

<https://angular.io/docs/ts/latest/> Angular 16

<https://www.typescriptlang.org/docs/> TypeScript

<https://tools.ietf.org/html/rfc7159> JSON

<https://www.w3.org/standards/webdesign/script> Javascript

2.2. Poslovna logika

Poslovna logika temelji na Jakarta EE standardu, izvaja se nad aplikacijskim strežnikom družine JBoss (WildFly 29). Predvidena je implementacija delilnika bremen na strojni stikalni opremi (izven domene tega projekta). Upravljevalec bo lahko dinamično povečal in manjšal število zalednih implementacij istega sklopa sistema z uporabo Kubernetes storitev. Strežba statičnih vsebin (html, javascript in slik) se prav tako izvaja v okviru Kubernetes, vendar ločeno od zalednih (API) storitev. Ločeni (izven Kubernetes) Apache ali NGINX strežniki v okolju naročnika niso predvideni. Takšen sistem omogoča izvedbo nadgradnje med delovanjem brez izpadov, tako imenovan rolling update (odvisno tudi od vrste spremembe).

Poslovna logika je izvedena kot stateless EJB storitev z REST vmesnikom in zaščito (avtentikacijo) OIDC z žetoni (Bearer JWT). Žetone s kratkim rokom trajanja (5 minut) izdaja centralni avtentikacijski sistem IS Monitoring SSO, ki temelji na odprtokodnem produktu Keycloak, ki je postavljen v obliki grozda. IS Monitoring SSO v produkcijski postavitvi le izjemoma sam izvaja avtentikacijo, čeprav je to v celoti podprto. Praviloma posreduje avtentikacijski zahtevek zunanji storitvi, ki bo v tem primeru skupni gradnik SI-CAS. Poslovna logika ne izvaja nobenega prometa v smeri IS Monitoring SSO za namene preverjanja sej. Veljavnost žetona se preverja izključno na podlagi veljavnosti podpisa v žetonu, ki ga od IS Monitoring SSO prejme brskalnik uporabnika. Tako ima IS Monitoring SSO privatni ključ (nastane vsakih 24 ur v IS Monitoring SSO in ga ni mogoče spremeniti). Vsaka postavitev poslovne logike ima med nastavitvami tudi javni ključ s katerim preverja ustreznost žetona in veljavnost. Zato je izrednega pomena usklajenost ur (čas) med vsemi instancami poslovnega dela sistema (nujna uporaba NTP ali primerljivega sistema). Pri tem je razumno odstopanje do 15 sekund. Uporabniški vmesnik je zavezan, da ne posreduje žetonov, ki jim bo veljavnost potekla čez manj kot 60 sekund. Za pot do poslovnega nivoja je preostalih 45 sekund dovolj. Trajanje samega zahtevka na poslovnem nivoju na to nima vpliva, saj se veljavnost žetona na poslovnem nivoju preverja takoj na začetku sprejema zahtevka. EJB storitev preverja veljavnost žetona implicitno (brez programske kode izvajalca), vloge pa deklarativno. Tako REST zahtevek, ki ni ustrezno avtentificiran in avtoriziran, ne pride do metode, ki jo naslavlja, temveč je zavržen na nivoju JBoss modula OIDC.



Omenjeno delovanje v praksi, če ni težav na avtentikacijskem sistemu, ne povzroča čakanja uporabnika, saj pridobi žeton v manj kot 20ms, kar je za uporabnika neopazno. In to seveda le takrat, ko je žeton tik pred potekom.

EJB storitev za dostop do podatkovne zbirke uporablja JDBC (z uporabo Oracle JDBC gonilnika), pred uporabo JDBC sistem za izbrane podatke (pogosto uporabljeni šifranti, avtorizacijske informacije o uporabniku) poskusi pridobiti podatke iz predpomnilnika. Predpomnilnik izbriše zapise največ 15 minut po prvem branju, kar omogoča posodabljanje šifrantov kljub uporabi predpomnilnika in brez restarta aplikacij.

Aplikacijski grozd povezuje aplikacijske strežnike v virtualnem omrežju (od zunaj ni dosegljiv), omrežje je implementirano na nivoju Kubernetes. Predvideno je eno takšno grozdno omrežje in sicer za IS Monitoring SSO. Tako je IS Monitoring SSO omrežno ločen od API in preprečuje napredne napade (na primer cache poisoning). Ostali moduli ne potrebujejo groznega omrežja temveč komunicirajo preko Kafka storitve.

Kadar podatkov v predpomnilniku ni, izvede sistem klic pripravljenega ukaza (prepared statement) brez lepljenja SQL stavkov (uporabljen je parameter binding). To zagotavlja varnost pred SQL injection. Za namene transakcijske obdelave podatkov so uporabljene PL/SQL procedure in funkcije. Za CRUD operacije (branje in pisanje) bazni uporabnik ne potrebuje dostopa do tabel ali pogledov. Za iskanje in analitiko so uporabljeni prilagojeni SQL (Select) ukazi implementirani na nivoju API. To pomeni, da za uporabo filtrov, iskalnikov in drugih dinamičnih pogledov na podatke, poslovni nivo pripravi SQL poizvedbo, pri čemer SQL poizvedbo gradi z metodo lepljenja nizov v obliki vnaprej pripravljenih segmentov. Obenem so vsi parametri poizvedbe brez izjeme predani v obliki parametrov (binding).

Storitev ima minimalen nabor pravic za dostop do PL/SQL paketov in v primeru iskalnikov in analitike tudi pogledov. PL/SQL paketi in pogledi so domensko izdelani, kar pomeni, da so namenjeni posamezni funkcionalnosti, ki jo tudi ustrezno ščitijo (minimalen nabor stolpcev in vrstic). Omejevanje vrstic se izvaja na podlagi prijave na podatkovno zbirko (s tem je enolično določeno za katero storitev gre in iz katerega varnostnega območja je vzpostavljena povezava). Omejevanje je izvedeno tudi na podlagi uporabnikovih vlog. Ta zaščita se izvaja na podatkovni zbirki vendar na podlagi informacije, ki jo posreduje poslovni nivo. Če ta informacija ni podana, bazni uporabnik ne vidi podatkov, čeprav ima dostop do metode.

Integracijski del sistema ne odstopa od ostalih delov sistema. Več o sistemu integracij je v poglavju 6 Integracije z zunanji sistemi. Implementiran je z uporabo čakalnih vrst, ki so shranjene na podatkovni zbirki in delavcev (workers) implementiranih v ločeni aplikaciji imenovani AsyncScheduler. Navedena aplikacija izkorišča sistem asinhronih procesov znotraj Wildfly, tako da omejuje število sočasnih procesov tako za interne asinhorne naloge informacijskega sistema kakor za naloge, ki presegajo meje informacijskega sistema in se zato imenujejo »integracije«.

Vhodni klici (iz drugih informacijskih sistemov) so implementirani enako kakor klici z uporabniškega vmesnika. Dokumentirani so z uporabo Swagger.

Za namene izdelave dokumentov na podlagi predlog bo uporabljeno orodje JasperReports, obvestila na elektronski naslov bodo posredovana z uporabo SMTP.

Uporabljeni so standardi http, REST, JSON, WebSocket, Jakarta EE, EJB, JAX-RS 2.1, SQL.

Specifikacije uporabljenih tehnologij:

<https://tools.ietf.org/html/rfc2068> http

<https://tools.ietf.org/html/rfc7231> http vsebina (REST)



<https://tools.ietf.org/html/rfc6455> WebSocket

<https://tools.ietf.org/html/rfc7159> JSON

<https://jakarta.ee/specifications/platform/10/> Jakarta EE Platform 10

<https://jakarta.ee/specifications/webprofile/10/> Jakarta EE Web Profile 10

<https://jakarta.ee/specifications/enterprise-beans/4.0/> Jakarta Enterprise Beans 4.0

<https://jakarta.ee/specifications/restful-ws/3.1/> Jakarta RESTful Web Services 3.1

in ostale specifikacije iz družine Jakarta EE 10

<http://www.contrib.andrew.cmu.edu/~shadow/sql/sql1992.txt> SQL-92

2.3. Kontejnerji

Uporaba kontejnerjev (v konkretnem primeru Kubernetes) je ključen element arhitekture aplikacij IS Monitoring. Šele z uporabo kontejnerjev pridejo do izraza odločitve pri gradnji arhitekture kot so stateless storitve, sistem enotne prijave (SSO), delitev bremena (load balancing), skalabilnost (razširljivost), odpornost (resilience), tekoče nadgradnje (rolling updates) itd.

Kapaciteta sistema (procesor, pomnilnik, disk) se združi (ne glede na število fizičnih ali virtualnih strežnikov) v eno storitveno gručo (Kubernetes cluster). V to gručo glede na izbrano politiko upravljaavec namešča storitve. Posamezna storitev vzpostavi vsaj eno instanco slike (image) implementacije, po potrebi pa tudi več in to je mogoče dinamično prilagajati obremenitvam sistema (scaling). Upravljaavec določi katera verzija posamezne storitve naj bo v uporabi in v koliko instancah, sistem poskrbi za ostalo.

Kontejnerji pa prinašajo tudi izzive. Ker ima vsako okolje svoje posebnosti in ker je nameščanje virtualnih strežnikov (tudi kontejnerjev), ki jih je izdelal zunanji izvajalec, varnostno sporno, je potrebno zagotoviti, da se slika (image) pripravi transparentno. Torej, da vsebuje le tiste datoteke in nastavitve, ki so v danem primeru smiselne in ne vnašajo varnostnih ranljivosti ali nestabilnosti. Končno sliko (image) zato izdelava upravljaavec sam, na podlagi besedilne specifikacije (Docker datoteka). Tako lahko prilagaja posamezne nastavitve kontejnerja, nameščene knjižnice in pakete, predvsem pa ohranja nadzor nad končno izdelano sliko. Takšna slika ne vsebuje specifičnih omrežnih nastavitvev ali uporabniških imen in gesel. Še vedno je dovolj generična, da jo je mogoče namestiti v testno okolje in po potrditvi ustreznosti tudi v produkcijsko. Razlike med navedenimi okolji so podane v fazi priprave storitve.

2.4. Podatkovni nivo

Vsi podatki sistema so hranjeni centralno v podatkovni zbirki sistema oziroma v povezanih zunanjih storitvah. Podatkovna zbirka sistema je Oracle Database Enterprise 19, ki je nameščena v okolju upravljavca. Zaradi lažjega upravljanja z večjo količino podatkov bo uporabljena opcija Partitioning. Opcija se uporabi na področju večjih sklopov podatkov smiselno, tako da zmanjša pritisk na pregledovanje velikih tabel in (ob večjih brisanjih) na podatkovne dnevnike. Dodatno ima podatkovna zbirka nameščene opcije Spatial, Oracle Text in XML DB (izključno zaradi objektov vrste XMLTYPE).

Podatkovna zbirka predstavlja centralno točko zagotavljanja integritete podatkov. Implementacija poslovnih pravil sledi ciljem pravilnosti delovanja in odzivnosti sistema.



Predvidena je uporaba enotne sheme za podatke IS Monitoring. Dodatno, po dogovoru z naročnikom, predvidevamo eno shemo, z imenom ISMON, skozi katero naročnik lahko izpostavi podatke (samo za branje) drugim sistemom znotraj naročnikovega informacijskega sistema.

Uporabljen je standard SQL.

<http://www.contrib.andrew.cmu.edu/~shadow/sql/sql1992.txt> SQL-92

2.5. Dokumentni nivo

Aplikacije IS Monitoring se bodo povezovale z obstoječim dokumentnim sistemom SPIS, ki je v uporabi na ARSO. Konkreten način integracije ni predmet tega dokumenta.

Znotraj aplikacij IS Monitoring bo omogočeno dodajanje dokumentov (npr. pdf) neposredno mimo obstoječega dokumentnega sistema SPIS. Za posamezen dokument se bodo v aplikacijah IS Monitoring (v podatkovni zbirki) poleg elektronske oblike dokumenta hranili tudi določeni atributni (meta) podatki (npr. tip dokumenta, datum izdaje in podobno).

V aplikacijah IS Monitoring je predvidena implementacija funkcionalnosti elektronskega podpisovanja dokumentov, za kar bo uporabljen sistem SI-CES (spletno podpisovanje).

Uporabljena sta standarda XML in ISO 19005-1 (PDF/A)

<https://www.w3.org/TR/2006/REC-xml11-20060816/> XML 1.1

<https://www.iso.org/standard/38920.html> 19005-1 (PDF/A)

3. Neprekinjena integracija in neprekinjena dostava/neprekinjeno uvajanje

Continuous integration and continuous delivery/continuous deployment

V skladu z dogovorom z naročnikom (ARSO) se CI/CD sistem vzpostavi pri naročniku, kjer se tako gradijo:

- Uporabniški vmesnik (Angular build)
- Predstavitveni nivo (Maven build)
- Izgradnja slik za kontejnerje (Docker build)

Vse skripte, torej tudi tiste, ki jih naročnik uporablja za CI/CD se vodijo v repozitoriju in so na voljo za vse deležnike projekta. Obenem so vse skrivne vsebine, kot na primer gesla in privatni ključ, implementirani z uporabo Kubernetes secrets in so edini objekti, ki jih je potrebno (in obenem dovoljeno) kreirati in spreminjati ročno na izvajalnem okolju. Vse ostale vsebine so skriptirane in del centralnega repozitorija.

Repozitorij centralno vzpostavi in vodi naročnik in izvajalec paralelno. Naročnik vzpostavi repozitorij, tako da omogoča prenos sprememb iz repozitorija izvajalca z uporabo registracije »remote« in »pull request«. Oblika je Git. Izvajalec naročniku omogoči dostop, tako da lahko naročnik sam, brez aktivnosti izvajalca, prevzema kodo in spremembe v namestitvenem procesu. Naročnik pripravi postopke prevzema, tako da je postopek sledljiv in ga lahko izvajajo tudi osebe,



ki jih naročnik pooblasti (na primer vodja projekta na strani naročnika). Naročnik zagotovi okolje za upravljanje z izgradnjo in nameščanjem, tako da je postopek sledljiv in ga lahko izvajajo tudi osebe, ki jih naročnik pooblasti (na primer vodja projekta na strani naročnika). Naročnik se prosto odloča ali bo dostop do naročnikovega repozitorija in okolja za upravljanje z izgradnjo in nameščanjem omogočil tudi izvajalcu in v kakšni meri. S tem pa seveda vpliva tudi na nivo podpore, ki jo izvajalec lahko izvaja (brez dostopa izvajalec ne more izvajati podpore oziroma je ta izjemno omejena).

Vodi se en centralni repozitorij (na dveh lokacijah – pri naročniku in izvajalcu), tako za izvorno kodo kakor namestitvene objekte.

Spremembe v tem repozitoriju izvajata naročnik in izvajalec, pri čemer neposreden commit v ključne veje (dev, test in prod) niso dovoljene. Dovoljena je izključno uporaba PR (pull-request). Dodatno se repozitorij po vsebini (mapah) deli na:

- Izvorno kodo
- Namestitvene objekte

3.1. Mape izvorne kode

V mapah izvorne kode je vsa koda za celoten projekt in vključuje vsaj:

- Kodo uporabniškega vmesnika
- Kodo zalednega sistema
- Kodo in skripte podatkovnega nivoja

Spremembe v teh mapah izvaja izključno izvajalec. Vse spremembe, vključno z objekti na podatkovni zbirki, ki so v shemah IS Monitoring izvaja izključno izvajalec. To omogoča popolno sledljivost spremembam, jasno razmejitev odgovornosti in posledično predvidljivo delovanje.

Izvajalec spremembe prenaša iz svojega okolja kot statične vsebine in jih označuje z značkami (tag), kadar naroča namestitve. Izgradnja se izvaja na naročnikovem CI/CD, pri čemer vse skripte in lastnosti naročnik in izvajalec vodita skupaj v ločenih mapah.

V repozitoriju izvajalec vodi vsaj dve veji:

- Prod, ki je edini vir iz katerega se pripravlja produkcijske verzije
- Test, ki je edini vir iz katerega se pripravlja testne verzije, ki je novejša verzija prod

Izvajalec po namestitvi produkcijske verzije izvede merge iz prod v test. Merge iz test v prod se ne izvaja in je **prepovedan**. Le v teoriji namreč vse spremembe iz testnega okolja končajo v produkcijskem okolju. Razlika med vejama prod in test služi kot evidenca razlik in ne kot izhodišče za pripravo verzij.

Oddaja (push) neposredno v vsako izmed navedenih vej je blokiran, za kar poskrbita naročnik in izvajalec, vsak na svojem okolju. Omogočena je izdelava ločenih (distribucijskih) vej in premikov (pull-request) iz distribucijskih vej v glavni veji. Distribucijske veje se izdelajo iz veje, v katero namenjamo spremembe.

Normalen tok za spremembo je torej, da izvajalec izdelava novo vejo iz prod veje, pripravi in odda spremembe, potem izvede premik (PR) v test vejo. Ko je pripravljen na oddajo v prod, izvede premik v prod vejo. Ko je sprememba v obeh glavnih vejah, lahko izvorno vejo pobriše.



Naročnik lahko omeji premik (PR) v prod vejo z namenom vzpostavitve potrjevanja sprememb s strani naročnika.

3.2. Mape namestitvenih objektov

V teh mapah so vse skripte in nastavitve za namestitev, kar vključuje reference na konkretne veje v repozitoriju izvirne kode. V CI/CD ni nastavitvev, ki bi skrivale poln nadzor procesa.

Naročnik omogoči proženje izgradnje iz značk (tags) in s tem namestitve aplikacij (vsaj v testno okolje) bodisi izvajalcu ali vodi projekta na strani naročnika.

Naročnik za nameščanje sprememb na **testno** podatkovno zbirko omogoča eno izmed variant:

- Namešča spremembe ročno in sicer sproti, to je v roku 24 ur od oddaje verzije. Termin je vnaprej usklajen med naročnikom in izvajalcem.
- Omogoči nameščanje izvajalcu
- Omogoči skriptirano nameščanje, zagotavljanje revizij in ostalih funkcionalnosti s katerimi je omogočanje nameščanje sprememb brez ročnih posegov.

Pravila za prenos sprememb so enaka pravilom za prenos sprememb izvirne kode.

Razlika je v tem, da v teh mapah naročnik lahko izvaja spremembe tudi sam, pri čemer spreminja le nastavitve, specifične za njegovo okolje, nikakor pa ne spreminja vsebin skript, saj morajo te iste skripte delovati tudi v okolju izvajalca.

4. Arhitektura sistema za implementacijo

Arhitektura IS Monitoring je prilagojena obstoječi informacijski arhitekturi na DRO z upoštevanjem specifičnih okoliščin ARSO in temelji na dokumentih »Smernice MJU za razvoj informacijskih rešitev« in »Generične tehnološke zahteve za razvoj informacijskih sistemov (GTZ)«.

Postavitev sistema temelji na izhodiščih:

- Visoka razpoložljivost
- Dinamična zmogljivost (skalabilnost)
- Varnost (šifrirane povezave)
- Odpornost (resilience)
- API brez stanja (stateless)
- Prilagodljiva uporabniška izkušnja (responsive design).

Podatkovna zbirka je ena, centralna in bo skupna za aplikacije IS Monitoring.

Za posamezne funkcionalnosti so predvideni ločeni API-ji.

Predvidena je implementacija delilnika bremen na strojni stikalni opremi. Zaledni sistemi so implementirani v stateless obliki. Upravljevec bo lahko dinamično povečal in manjšal število zalednih implementacij istega sklopa sistema. Strežba statičnih vsebin (html, javascript in slik) se izvede znotraj ločenih Kubernetes storitev. Na nivoju Kubernetes se izvede tudi usmerjanje prometa na zaledne API sisteme na podlagi url (context). Zato Apache ali NGINX strežniki v testni in produkcijski postavitvi niso predvideni.



Predvidena je uporaba JBoss Wildfly 29 v obliki Docker kontejnerjev. Pri tem bodo izdelki zgrajeni v okolju ARSO, tako bo ARSO imel končno kontrolo nad vsebino izdelkov. Posebej to velja za docker kontejnerje, kjer velja, da bo definicija kontejnerja del Git, kontejner izgradi CI/CD v okolju ARSO. Na tak način bo produkcijsko, testno in razvojno okolje bolj usklajeno. Varnostno občutljivi podatki (na primer gesla, ključi ipd.) niso predmet image definicije, temveč jih upravljaavec določa ob namestitvi. Enako velja za vse mrežne nastavitve in načrtovane razlike med okolji (testno, šolsko, produkcijsko).

5. Varnostni in zaščitni mehanizmi

Podrobnosti o profilih uporabnikov so na voljo v poglavju 0 [Pod temi krovnimi vlogami je večje število uporabniških vlog, ki pokrivajo posamezne funkcionalne sklope in so izven konteksta tega poglavja. Uporabniške vloge bodo bolj podrobno opisane v vsebinskih analizah.](#)

~~Profili Pod temi krovnimi vlogami je večje število uporabniških vlog, ki pokrivajo posamezne funkcionalne sklope in so izven konteksta tega poglavja. Uporabniške vloge bodo bolj podrobno opisane v vsebinskih analizah.~~

~~Profili.~~

Vsebina tega dokumenta temelji na podatkih o profilih uporabnikov, na tem mestu je zapisan le povzetek:

- Več kakor 3.000 (ocena naročnika presega 10.000) uporabnikov od tega 30 uporabnikov, ki do sistema dostopajo znotraj HKOM
- Več različnih poslovnih procesov, od katerih je večina dostopna uporabnikom znotraj in izven HKOM v polnem obsegu

Varnostni in zaščitni mehanizmi so bistveni del vsakega sistema, tako tudi IS Monitoring, ker zagotavljajo varnost na vseh nivojih (arhitekturni, sistemski, podatkovni).

5.1. Arhitekturni nivo

5.2. Zaščita komunikacijskih kanalov

Aplikacije IS Monitoring ne implementirajo zaščite komunikacijskih kanalov, ampak to funkcijo izvaja naročnik s specifično opremo pred IS Monitoring. Uporabljena je šifrirana varna povezava (SSL) med uporabnikovim brskalnikom in dostopno točko v okviru ARSO. Sistem uporablja enotno dostopno točko (zmanjševanje profila za napad) za dostop znotraj ARSO in eno za dostop izven ARSO, pri čemer v obeh primerih na enakem DNS naslovu, za usmerjanje glede na okolje pa naročnik uporabi split-DNS koncept.

Naročniku predlagamo, da za IS Monitoring uporabi naslov ismonitoring.arso.gov.si in s tem povezan <https://ismonitoring.arso.gov.si>

Naročnik bo z IS Monitoring pridobil tudi močno orodje za združevanje različnih mehanizmov avtentikacije v obliki IS Monitoring SSO. Izvajalec predvideva postavitve tega podsistema na istem spletnem naslovu kot ostale aplikacije IS Monitoring.

V preteklosti se je pogosto izkazalo, da je naročnik kasneje takšno rešitev uporabil kot centralno rešitev v svojem informacijskem okolju, torej tudi za druge informacijske sisteme. V tem primeru naročniku predlagamo, da za to storitev rezervira naslov auth.arso.gov.si in s tem povezan <https://auth.arso.gov.si>



Povezave med dostopno točko in storitvami niso šifrirane.

Uporaba sodobnih sistemov šifriranja (algoritmi in dolžina ključev) onemogoča uporabo starejših brskalnikov, ki niso več vzdrževani s strani proizvajalcev.

5.3. Sistemski nivo

Vsi elementi aplikacij IS Monitoring zaupajo IS Monitoring SSO gruči z uporabo standardnega OIDC protokola. Vsak uporabnik (tudi klienti storitev API) se avtentificirajo na IS Monitoring SSO. IS Monitoring SSO izda JWT žeton, ki je podpisan, kar je veljavno dokazilo za vse aplikacijske strežnike. IS Monitoring SSO je redko samostojen v izvedbi avtentikacije (le kadar bi bil uporabljen mehanizem user/password). Praviloma zahtevo za avtentikacijo posreduje tretjim gradnikom (v primeru IS Monitoring sistem bo to SI-CAS).

Do sistema lahko dostopajo uporabniki s kvalificiranim digitalnim potrdilom, ki je veljaven v Republiki Sloveniji, lahko pa se naročnik in skrbnik SI-CAS odločita tudi drugače in omogočita ostale mehanizme (na primer SMS-PASS, osebna izkaznica itd). Uporabniki se identificirajo v sistemu SI-CAS/SI-PASS. Dostop je omogočen tudi za sisteme, ki jim je Monitoring pred tem določil trajni žeton za izvedbo avtentikacije. Uporaba uporabniškega imena in gesla v produkcijskem okolju ni predvidena. Po končani uspešni avtentikaciji sistem uporabniku v žeton doda krovne pravice za dostop do aplikacij IS Monitoring glede na uporabniške pravice.

IS Monitoring SSO uporablja ločeno povezavo na podatkovno zbirko. Povezava omogoča branje in za urejanje uporabnikov, shranjevanje zgodovine prijav in dodeljenih pravic uporablja CRUD stavke (nad pogledi).

Aplikacija ob dostopu preveri, ali ima uporabnik na voljo žeton za varovanje sistema. Praviloma takšnega žetona nima (razen, ko odpre nov listič v brskalniku), zato ga aplikacija preusmeri na centralni avtentikacijski sistem IS Monitoring SSO. Po zaključeni avtorizaciji (bodisi interno v IS Monitoring SSO ali po posredovanju na zunanjo storitev) IS Monitoring SSO uporabnikov brskalnik preusmeri nazaj na aplikacijo z uporabo globokih povezav (deep link) in z žetonom za varovanje sistema. Tako uporabnik lahko dostopa do konkretne vsebine v sistemu (in ne izključno do začetne strani). Aplikacija ob vsakem zahtevku do poslovnega nivoja poda žeton kot del zahtevka. Ker ima žeton izredno kratko veljavnost (5 minut), aplikacija pred vsakim dostopom preveri starost žetona in po potrebi (če je starejši od štirih minut) na IS Monitoring SSO izda zahtevek za osvežitev žetona (z uporabo klica REST). Tako uporabniku ni treba izvajati ponovne prijave vsakih 5 minut, sistem pa je varovan z vedno svežim žetonom. Zaradi časovne omejenosti trajanja žetona je pomembna časovna usklajenost uporabnikovega sistema s centralnim sistemom.

5.4. Omejevanje dostopa

Uporabnik vidi le funkcionalnosti, ki jih ima na voljo glede na dodeljene pravice. To velja tako za menijsko strukturo, kakor funkcionalne elemente (gumbi, meniji,...) znotraj posameznega konteksta.

Prav tako nima na voljo dostopa in s tem prikaza do subjektov, do katerih nima pravic.

Vizualno omejevanje je implementirano večinoma v aplikaciji v brskalniku, zato je le dodaten element, ki pa ne predstavlja varnostnega mehanizma v smislu varovanja podatkov pred zlorabo. Omogoča pa, da uporabniku ne izpostavimo pogleda na funkcionalnosti, ki jih ne sme uporabljati in tako skrijemo tudi del sistema, ki bi ga lahko napadel.



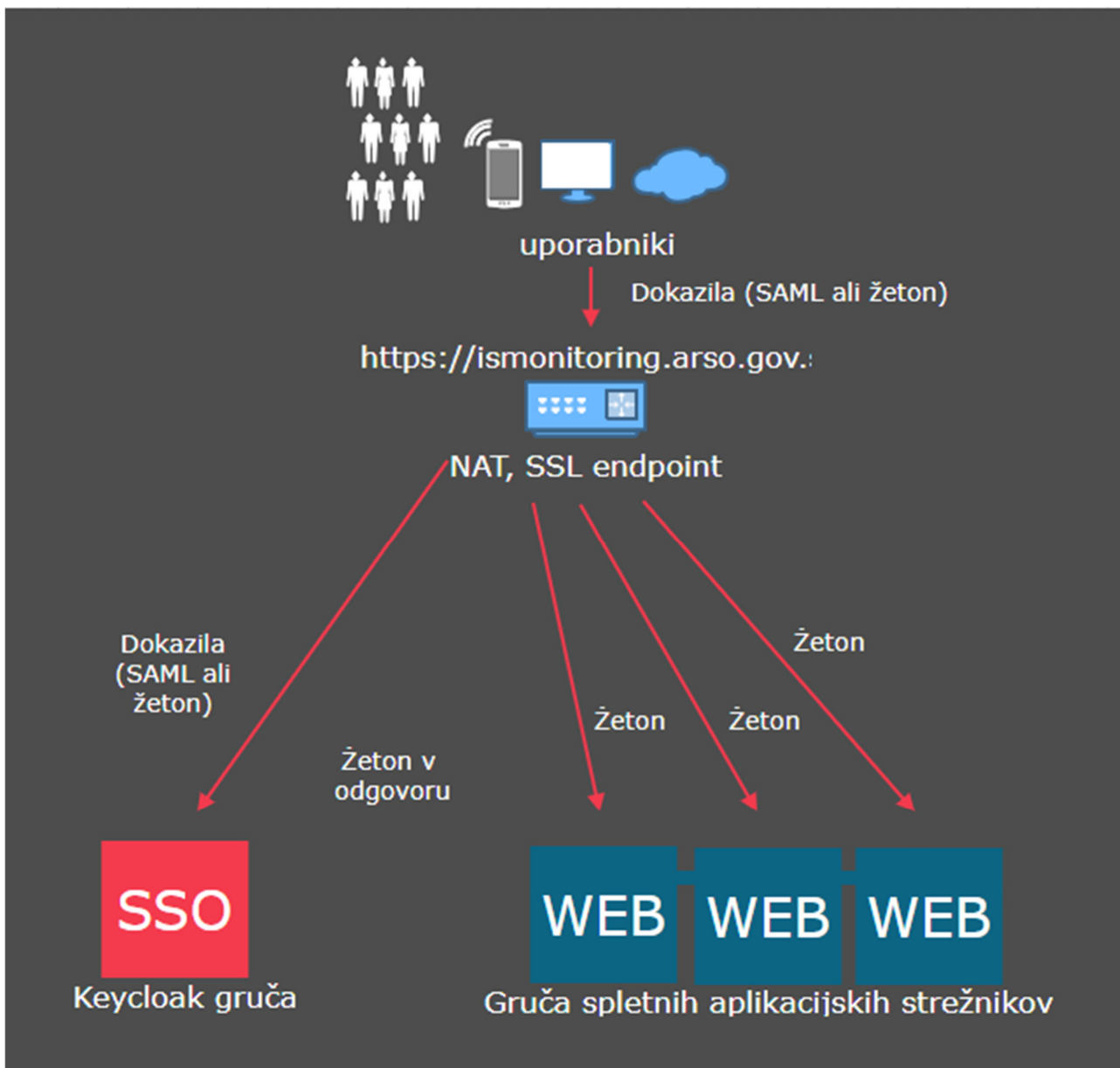
Uporabniške pravice (role) kreira skrbnik aplikacij IS Monitoring. Šifranti vlog in pravic se polnijo z verzijami preko alter skript.

Aplikacije IS Monitoring ne omogočajo urejanja in dodeljevanja uporabniških pravic nad uporabnikom, prav tako jih ne shranjujejo. Urejanje in dodeljevanje uporabniških pravic nad uporabnikom se izvaja izključno v ločenem avtorizacijskem sistemu IS Monitoring. Aplikacije IS Monitoring pridobijo seznam uporabnikovih pravic iz enotne podatkovne zbirke IS Monitoring.

Aplikacije IS Monitoring imajo zato pravice branja nad tabelami avtorizacijskega sistema.

5.5. Zaščita pred tretjimi osebami

Zaščita pred tretjimi osebami je zaščita pred osebami, ki niso uporabniki IS Monitoring.



Slika 2: Izmenjava dokazil med uporabnikovim brskalnikom in elementi sistema IS Monitoring.

Vsaka izmed storitev IS Monitoring pričakuje, da uporabniška zahteva s seboj prinaša dokazilo o pristnosti. Vse storitve razen SSO podsistema IS Monitoring SSO zahtevajo, da je takšno dokazilo o pristnosti veljaven OpenId žeton, ki ga izda SSO podsistem.

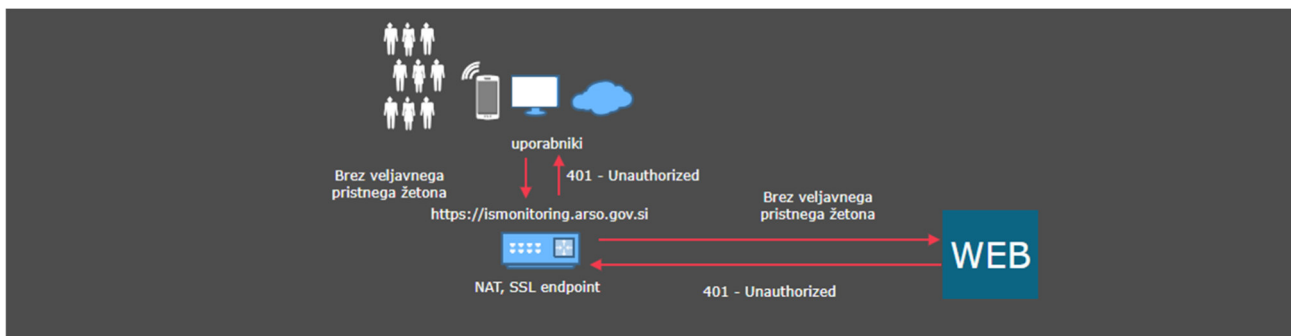


SSO podsistem IS Monitoring SSO izda JWT žeton na podlagi dokazil uporabnika. Dokazilo je lahko obstoječ veljaven žeton (uporabnik je že prijavljen) ali dokazilo, ki je določeno v fazi načrtovanja sistema (SI-CAS, trajni žetoni za druge IS). IS Monitoring SSO podpira več načinov avtentikacije uporabnika (LDAP, Active Directory, uporabniško ime/geslo, uporabniško kvalificirano digitalno potrdilo, zunanja SSO storitev itd). Ob tem je lahko aktivnih več načinov avtentikacije hkrati. V kontekstu IS Monitoring se v produkcijskem okolju uporablja izključno SAML zunanja storitev (SI-CAS) in trajni žeton. V testnem okolju se poleg navedenih uporablja še uporabniško ime in geslo zaradi zagotavljanja visoke razpoložljivosti (testni sistem SI-CAS ne zagotavlja enake razpoložljivosti kakor produkcijski).

Žeton, ki ga izda SSO je podpisan s privatnim ključem, ki je poznan izključno IS Monitoring SSO in se menja vsakih 24 ur. Tako je zagotovljena avtentičnost dokazila. Javni ključ je dostopen na javnem naslovu predvsem z namenom preverjanja s strani aplikacij IS Monitoring. Žeton ima tudi izredno kratko veljavnost (5 minut). V obdobju veljavnosti seje lahko uporabnikov brskalnik zahteva izdajo novega žetona, ki ima prav tako veljavnost 5 minut. Tako od uporabnika v času aktivnosti sistem ne zahteva ponovne prijave, po drugi strani pa je mogoče omejiti veljavnost seje v primeru sprememb ali potrebe po odklopu uporabnikov.

Vsaka izmed storitev pričakuje, da uporabniška zahteva v glavi zahtevka (Authorization header) poda žeton. Pristnost žetona preverja z uporabo javnega ključa IS Monitoring SSO. Storitev tako ne izvaja nobene komunikacije z SSO, razen pridobivanja podpisnega javnega ključa. Vsebina žetona storitvi prenaša identiteto uporabnika (v obliki tehničnega identifikatorja - GUID), poleg tega pa še nastavljive podatke; privzeto ime, priimek, e-mail in krovne vloge, ki so podrobneje opisane v poglavju 7.4 Krovne vloge. Če žeton ni podan ali ni pristen ali mu je potekla veljavnost, storitev odgovori s 401 – Not Authorized, brez podrobnosti. Storitev ne izdaja nikakršnih preusmeritev (redirect). To je tudi ključni element zaščite pred tretjimi osebami.

Storitev za posamezno povezavo ne kreira seje na strežniškem nivoju. Vse podatke pridobi iz žetona ali podatkovne baze (te podatke sistem hrani tudi v predpomnilniku). Na ta način zmanjšamo pomnilniški odtis, omogočimo tudi pravi stateless storitveni nivo.



Slika 3: Storitve zavračajo zahtevke brez veljavnega pristnega žetona (v odgovoru ni podrobnosti o razlogu zavrnitve).

Pošiljanje veljavnega žetona je tako naloga aplikacije, ki teče v brskalniku uporabnika. Ta aplikacija prav tako preverja veljavnost žetona (v tem primeru brez javnega ključa – z namenom zaščite pred brute-force napadi na mehanizem podpisa). V primeru, da žetona aplikacija nima ali je žeton tik pred potekom (manj kot 1 minuta do poteka), aplikacija izvede zahtevek na SSO za podaljšanje in dobi nov žeton. Operacija je za uporabnika transparentna. **Pogoj je usklajenost ure med storitvami in SSO sistemom z uporabo NTP ali primerljivega koncepta!**



Uporabnikov brskalnik lahko aplikacijo pridobi brez dokazil, dosegljiva je na javnem naslovu kot statična vsebina. Ob zagonu v brskalniku aplikacija ugotovi, da žetona nima (tega hrani v pomnilniku brskalnika, ob zagonu aplikacije je ta prazen) in uporabnikov brskalnik preusmeri na SSO stran. S tem se aplikacija zapre, uporabnik je na SSO strani, kjer mora (glede na nastavitve sistema) izkazati svojo pristnost. Ko dokaže svojo pristnost, SSO brskalniku vrne navodila za preusmeritev na aplikacijo skupaj z žetonom. Tokrat aplikacija ob zagonu ugotovi, da ima žeton in lahko nadaljuje z delom.

Centralna pozicija sistema IS Monitoring SSO predstavlja enotno točko varovanja sistema. Potvarjanje žetonov (bodisi z vdorom v SSO sistem ali s krajo podpisnega ključa) predstavlja največjo grožnjo sistemu. Posamezna storitev je prav tako lahko tarča vdora, vendar je v tem primeru nabor podatkov, ki so ogroženi, ustrezno manjši. Varovanje SSO sistema je zato ključnega pomena za varnost sistema. To pomeni tako nadzor delovanja kakor sprotno posodabljanje! Naročnik mora zato načrtovati redna naročila za posodabljanje varnostnih mehanizmov sistema (običajno nekajkrat letno, ob objavljenih ranljivostih pa tudi izredno).

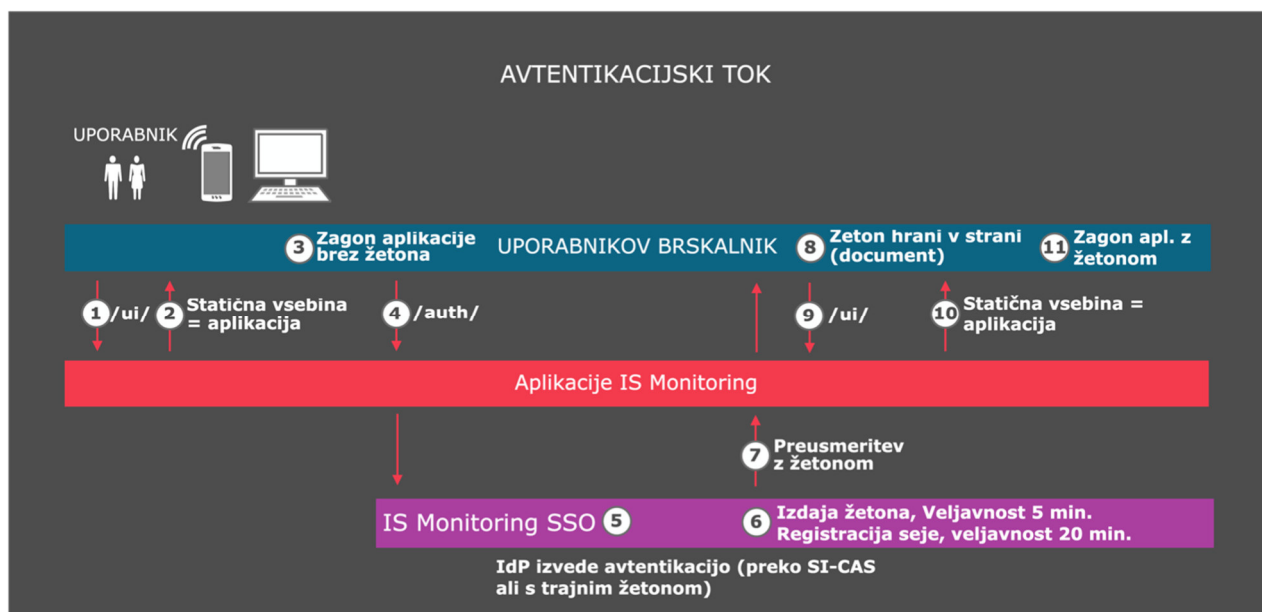
V primeru vdora v sistem je potrebno zagotoviti, da je ogrožen čim manjši del podatkov in postopkov, zato je smiselno ločevanje na zunanji (DMZ) in notranji del sistema, kadar je v sistemu nabor funkcionalnosti, ki je smislen le za notranje uporabnike. Skupaj z naročnikom smo ugotovili, da v IS Monitoring takih vsebin ni, zato je načrtovana ena postavitev s celotnim naborom funkcionalnosti, v DMZ.

5.6. Avtentikacija uporabnikov

Avtentikacijski sistem temelji na uporabi podatkov, ki jih vsebuje avtentikacijski sistem IS Monitoring SSO in predvideva možnost prijave v sistem na tri načine:

- Z uporabniškim imenom (ali elektronskim naslovom) in geslom (izključno v razvojnem in testnem okolju).
- Preko sistema SI-CAS in s tem vseh mehanizmov za katere se dogovorita ARSO in MDP
- Preko trajnih žetonov, ki jih IS Monitoring SSO izda tretjim storitvam za namen integracije

Potek prijave (authentication flow) v razmerju med uporabnikovim brskalnikom in sistemom IS Monitoring je prikazan na spodnji sliki.



Slika 4: Potek prijave v razmerju uporabnik - IS Monitoring

Glede na zgornjo sliko pri koraku 5 uporabnik izkaže svojo identiteto, v zgornjo sliko se vrne v koraku 6.

Veljavnost žetona je omejena na 5 minut. Daljše trajanje bi onemogočalo centralno upravljanje s sistemom, ker na primer uporabniku lahko odvzamete vse pravice, vendar bi uporabnik, ki je že prijavljen z aktivno uporabo sistema izvajal naloge v nedogled. Žeton se zato v aplikaciji (v ozadju) osvežuje, dokler je njegova prijava veljavna. Proces je prikazan na spodnji sliki.



Slika 5: Osveževanje dostopnega žetona



5.7. Avtentikacija zunanjih sistemov

Zunanji sistemi, ki dostopajo do IS Monitoring, uporabijo trajen žeton, ki ga izda IS Monitoring, s katerim od IS Monitoring SSO pridobijo dostopni žeton, ki velja 5 minut in s katerim lahko dostopa do storitev IS Monitoring.

V primerjavi z ostalimi uporabniki je torej razlika zgolj v tem, da ostale uporabnike IS Monitoring SSO preusmeri na SI-CAS, kjer izkažejo svojo istovetnost, zunanje storitve pa imajo trajen žeton, s katerim imajo vzpostavljeno trajno zaupanje v IS Monitoring SSO. Dolžnost vsake zunanje storitve je, da trajne in dostopne žetone hranijo varno in zaupno. Ta odgovornost je na strani zunanje storitve na kar jih mora naročnik IS Monitoring ob izdaji trajnega žetona nujno opozoriti.

5.8. Podatkovni nivo

Vsi dostopi do podatkovne zbirke so implementirani preko klicev namenskega nivoja spletnih storitev.

Dodatno so vse operacije sprememb podatkov in večina operacij branja podatkov izvedene z uporabo PLSQL paketov (stored procedure). Izjema so:

- funkcionalni sklopi, ki so izvedeni v obliki produktov (IS Monitoring SSO) in
- funkcionalni sklopi, kjer je zahtevana dinamična priprava poizvedb (analitika, iskanje z uporabo filtrov).

V vsakem primeru je dostop omejen preko posebnih pogledov, ki uporabnika na podatkovni zbirki omejujejo pri dostopu do podatkov, tako da pod nobenimi pogoji (tudi select brez where kriterijev) ne more dostopati do tabel, vrstic in stolpcev do katerih zunanji uporabniki nimajo dostopa (z uporabo Oracle RLS ali where kriterijev ali oboje).

Na podatkovni zbirki so izdelani namenski uporabniki za dostop posamezne storitve. Ti uporabniki imajo minimalen nabor konkretnih pravic in nimajo možnosti spreminjanja modela podatkovne zbirke. Zadnja linija zaščite je uporaba Oracle RLS, ki po omejitvah (stolpci in vrstice), ki jih ima prijavljeni bazni uporabnik, aplicira še omejitve končnega uporabnika (vloge in dostopi). Brez informacije o končnem uporabniku metode in pogledi na podatkovni zbirki za poglede, zaščitene z RLS, ne vračajo podatkov.

6. Integracije z zunanjimi sistemi

IS Monitoring se povezuje z različnimi sistemi. S sistemi izven ARSO (na primer IS Dovoljenja – IS za izdajo okoljevarstvenih dovoljenj, ki je v upravljanju MOPE) se implementirajo integracije z uporabo API. S sistemi, ki živijo znotraj ARSO, lahko naročnik sprejme odločitve za integracijo preko podatkovne zbirke (na primer KALIS).

6.1. Integracije preko podatkovne zbirke

IS Monitoring ima na podatkovni zbirki enotno shemo MON. Poleg te sheme je del IS Monitoring še shema INTEGMON. Shema MON:

- Nikoli in pod nobenim pogojem ne dostopa neposredno do drugih shem, z izjemo INTEGMON.
- Nikoli in pod nobenim pogojem ne daje dostopa neposredno drugim shemam, z izjemo INTEGMON.



6.1.1. Podatki so izvorno v IS Monitoring

Kadar so podatki izvorno v IS Monitoring, torej je v IS Monitoring tabela, ki je »single-point-of-truth« in te podatke uporabljajo še drugi sistemi, bo v INTEGMON izdelan pogled za branje (read-only view), ki ga ARSO po svoji presoji dovoli v uporabo drugim IS. Pogled se vzdržuje izključno v okviru IS Monitoring.

Kadar podatke poleg IS Monitoring spreminja še kak drug IS, bo v INTEGMON izdelan PLSQL paket s konkretnimi metodami, ki jih tak IS potrebuje. Paket bo izdelan specifično za konkreten IS in se uporablja le za ta IS. Paket se vzdržuje izključno v okviru IS Monitoring. Paket interno ne zaključuje transakcij.

6.1.2. Podatki so izvorno izven IS Monitoring

Kadar so podatki izvorno izven IS Monitoring, torej je izven IS Monitoring tabela, ki je »single-point-of-truth« in te podatke uporabljajo tudi IS Monitoring, bo v INTEGMON izdelan pogled, preko katerega IS Monitoring dostopa do teh podatkov. Pogled se vzdržuje izključno v okviru IS Monitoring.

Če je za integracijo potrebna uporaba PLSQL klicev, bo na shemi INTEGMON izdelan paket, preko katerega IS Monitoring izvaja klice na izvirne metode. Paket se vzdržuje izključno v okviru IS Monitoring. Paket interno ne zaključuje transakcij.

6.2. Integracije z uporabo API

Integracije z zunanjimi sistemi so v IS Monitoring implementirane znotraj API vmesnikov in jih ločujemo na:

- Integracije, kjer ima IS Monitoring vlogo klicatelja in
- Integracije, kjer ima IS Monitoring vlogo čakajočega na klic.

Pri razumevanju delovanja integracij je zelo pomembno ločevanje podatkovnega toka od komunikacijskega toka. Podatkovni tok bi na primer v razmerju med IS Dovoljenja in IS Monitoring v večini potekal od IS Dovoljenja proti IS Monitoring. Komunikacijski tok je od tega neodvisen in se lahko implementira, tako da klic začne IS Dovoljenja ali IS Monitoring in je povsem tehnična odločitev. V primeru integracij enakih podatkov z večimi IS, se tehnično pogosto sprejme bolj optimalna odločitev, to je, da je klicatelj več, kakor je čakajočih na klic. Tehnično je namreč bistveno težje urediti sistem, na katerem pričakujemo klice kakor sistem klicatelja. To je enostavno razumljivo, če primerjamo težavnost konfiguracije strežnika za spletno aplikacijo v primerjavi z brskalnikom, ki klic izvaja.

Po drugi strani praviloma tisti, ki čaka na klic, določa tehnična pravila integracije, kot na primer protokole (REST, Webservice, SOAP itd), avtentikacijo itd.

Obstaja še tretji vidik in ta je, da v večini primerov IS, ki izmenjujejo podatke, niso v isti fazi razvoja in zato eden izmed njih implementira integracijo, čeprav drugi še niso v fazi implementacije. V takšnih primerih praviloma prvi sistem implementira vlogo čakajočega na klic, če ne obstajajo drugi dobri razlogi za drugačno odločitev.

6.2.1. Iniciator klicev

Klici se lahko inicirajo:

1. Izven IS Monitoring
2. Znotraj IS Monitoring, neposredno na zahtevo uporabnika, sinhrono



3.Znotraj IS Monitoring, bodisi posredno na zahtevo uporabnika, asinhrono ali na časovni sprožilec

V zadnjem primeru se klici inicirajo znotraj API za asinhrono postopke, torej skozi vrste na podatkovni zbirki, ki jih API izvede ob ustreznem času.

6.2.2. Integracije, kjer ima IS Monitoring vlogo klicatelja

V primerih, kjer ima IS Monitoring vlogo klicatelja, se implementira integracija v vsebinsko primernem API ali API za asinhrono postopke, glede na to, kako se inicira klic (glej 6.2.1 Iniciator klicev).

V teh primerih, ker je IS Monitoring klicatelj, pravila integracije praviloma določa druga stran, torej prejemnik klicev. Ne glede na to obstajajo tehnične omejitve:

- Integracije se izvedejo izključno po HTTP(S) protokolu z izjemo integracij neposredno preko tabel in pogledov na podatkovni zbirki
- Ciljni naslov mora biti dosegljiv neposredno iz API ali preko HTTP Proxy.
- API mora imeti dostop do vseh podatkov (skrivnosti), ki so potrebne za dostop do storitev
- Uporabljeni so trenutno priznani in veljavni standardi (protokoli, enkripcija itd).

Skrivnosti (gesla, privatni ključ) se hranijo v Kubernetes secrets in so izvajalnemu okolju na voljo kot environment spremenljivka.

Predvidoma se vse takšne integracije izvedejo preko enega izmed protokolov:

- REST (IS Monitoring preferira ta protokol)
- WebServices
- SOAP

6.2.3. Integracije, kjer ima IS Monitoring vlogo čakajočega na klic

V primerih kjer ima IS Monitoring vlogo čakajočega na klic, se implementira integracija v vsebinsko primernem API in praviloma z uporabo REST ali, kadar gre za vsebinsko primerljivo vsebino, s souporabo API za uporabniški vmesnik. Vse vmesnike, ki so namenjeni za integracijo se opremi s Swagger anotacijami in ustrezno dokumentacijo. Avtentikacija se izvede enotno z ostalimi točkami dostopa z uporabo OIDC. V primeru dostopa s strani storitev (drugih aplikacij) se v IS Monitoring SSO ročno izdela klienta za posamezno zunanjo storitev. Storitve mora (skladno z OIDC) žeton, ob dostopu, uporabiti, tako da pridobi začasen »access« žeton, s katerim nato izvede klic na storitev znotraj IS Monitoring.

6.2.4. Integracija z IS Dovoljenja

Za potrebe izmenjav šifrantov in evidenc se IS Monitoring integrira z IS Dovoljenja preko REST API klicev. Za klic storitev IS Dovoljenja je potrebna avtentikacija v IS Dovoljenja SSO, ki je urejena z prijavo v klienta. Ob prijavi aplikacija pridobi začasen »access« žeton, s katerim nato izvede klic storitev na IS Dovoljenja. Izmenjava se proži, bodisi ob prejetem Kafka sporočilu o spremembi, bodisi na časovni sprožilec v sklopu asinhronih postopkov, ki skrbijo za izmenjavo šifrantov. Enako velja v drugo smer.

Za potrebe pravilnega delovanja izmenjave je potrebno urediti tudi:

- izmenjava ključev, ki se zapišejo med skrivnosti
- odprtje omrežnih poti



7. Upravljanje z uporabniki

7.1. Tehnični administratorji IS Monitoring SSO

Prvi uporabnik, ki je registriran v centralnem avtentikacijskem sistemu IS Monitoring SSO, je uporabnik »admin«, ki nastane v procesu namestitve IS Monitoring SSO. Geslo uporabnika določi administrator, ki namešča sistem. Koordinator sistema IS Monitoring lahko nato omenjenega uporabnika uporabi za pripravo drugih uporabnikov (z vlogo administrator) in nato onemogoči uporabnika »admin«. To je tudi proces, ki ga priporočamo naročniku. Tehnične administratorje koordinator izdelava poimensko, zato ne gre za generične uporabniške račune, ki jih uporablja več posameznikov. Dodelijo se zgolj tistim posameznikom, ki res upravljajo s sistemom in te dostope potrebujejo. Priporočljivo je da je takih uporabnikom čim manj, odločitev pa je na strani naročnika. **Teh računov ni mogoče uporabiti za prijavo v aplikacije IS Monitoring, temveč zgolj za upravljanje z IS Monitoring SSO in so zato posebej občutljivi na vdore.**

Upravljanje s temi uporabniki se izvaja neposredno v IS Monitoring SSO.

7.2. Registracija novih uporabnikov aplikacij IS Monitoring

Novi uporabniki aplikacije IS Monitoring se lahko registrirajo izključno preko IS Monitoring SSO. Obstajajo naslednji načini za registracijo novih uporabnikov:

- Z uporabo zunanje storitve SI-CAS
- Z ročno registracijo zunanje storitve
- Z ročno registracijo uporabnika, ki uporablja uporabniško ime in geslo (**onemogočeno za produkcijsko okolje**)

7.2.1. Registracija z uporabo zunanje storitve SI-CAS

Uporabnikov v IS Monitoring ne dodajamo ročno, ampak se dodajo avtomatsko ob uporabnikovem prvem uspešnem dostopu. Naloga administratorja je nato uporabnikom dodeliti ustrezne vloge (pravice), kar lahko uredi ročno (več v poglavju 7.6) ali preko potrditve uporabnikovega zahtevka za dodelitev dostopa (več v poglavju 7.3)

Proces poteka, tako da:

1. Uporabnik preko brskalnika dostopa do spletnega naslova, kjer se nahaja aplikacija IS Monitoring.
2. Sistem ugotovi, da uporabnik nima aktivne seje, zato ga preusmeri na IS Monitoring SSO.
3. Na IS Monitoring je v produkcijskem okolju na voljo zgolj prijava skozi SI-CAS, zato ga IS Monitoring SSO, tako kot vsakega, ki nima aktivne seje, preusmeri na SI-CAS.



4. Na SI-CAS uporabnik izkaže svojo identiteto z enim izmed načinov, za katere se dogovorita ARSO in MDP, predvidoma pa vsaj z enim izmed načinov na spodnji sliki:



Slika 6: Prijavno okno na SI-CAS

5. SI-CAS uporabnika skupaj s podatki o uporabniku (ime, priimek, e-poštni naslov, kvalificirano potrdilo, če ga je uporabnik uporabil ob prijavi, in sicas-id, kar je interni enolični identifikator SI-CAS), posreduje nazaj na IS Monitoring SSO.
6. IS Monitoring SSO preveri, ali je tak uporabnik že registriran. Za ugotavljanje uporabi naslednje mehanizme:
- Ali obstaja uporabnik s tem sicas-id? Sicas-id je interni identifikator SI-CAS, ki se ne spreminja, tudi če uporabnik uporabi drug mehanizem prijave (na primer enkrat uporabi Kvalificirano potrdilo, naslednjič pa smsPASS). Identifikator sicas-id se spremeni, če uporabnik pobriše profil na SI-CAS. Če obstaja uporabnik s tem sicas-id, ga poveže (posodobi podatke o uporabniku v IS Monitoring SSO). S tem uporabnik obdrži že dodeljene pravice in se ta proces zaključi. Če uporabnik ne obstaja, se postopek nadaljuje v naslednjem koraku.
 - Ali obstaja uporabnik s tem kvalificiranim potrdilom? V primeru, da sicas-id ne pozna, preveri, ali je SI-CAS poleg prijave priložil tudi kvalificirano potrdilo. V tem primeru preveri v interni evidenci IS Monitoring SSO, ali je uporabnik že kdaj dostopal do IS Monitoring s priloženim potrdilom. Če obstaja uporabnik s tem potrdilom, ga poveže (posodobi podatke o uporabniku v IS Monitoring SSO). S tem uporabnik obdrži že dodeljene pravice in ta se postopek zaključi.
 - Ali obstaja uporabnik s tem e-poštnim naslovom? V primeru, da sicas-id ne pozna in enako ne pozna kvalificiranega potrdila (ali pa to ni priloženo prijavi), preveri e-poštni naslov, ki ga je SI-CAS priložil poleg prijave. Preveri v interni evidenci IS Monitoring SSO, ali je takšen uporabnik že kdaj dostopal do IS Monitoring. Če obstaja uporabnik s tem e-poštnim naslovom, uporabnika blokira in s tem prepreči prevzemanje dodeljenih vlog. S tem se proces zaključi. Razreševanje blokirane uporabnika je prepuščeno administratorju. Če tak uporabnik ne obstaja, se postopek nadaljuje v naslednjem koraku.
 - Uporabnik v IS Monitoring SSO torej ni registriran, zato SSO ustvari nov zapis v evidenci uporabnikov, pri tem uporabi podatke, ki jih je prejel iz SI-CAS in



- uporabniku dodeli enolični identifikator v IS Monitoring SSO, ki je v obliki I12345678. Črka I v tem primeru predstavlja identiteto.
- e. Razen v primeru c, kjer uporabnika blokira, je v tej točki uporabnik prijavljen in registriran, poznamo njegovo identiteto, uporabnik je vpisan v evidenco in ima tudi enolični identifikator. S tem je postopek avtentikacije zaključen. IS Monitoring SSO uporabnika preusmeri nazaj v aplikacijo IS Monitoring, kjer je uporabnik začel postopek avtentikacije. Aplikacija IS Monitoring preveri ali ima uporabnik dostope (pravice ali vloge) v aplikaciji. Do te točke lahko namreč dostopa vsak, ki ima račun v SI-CAS in enega izmed dovoljenih načinov prijave. IS Monitoring v tem koraku preveri ali ima uporabnik kakšno izmed krovnih vlog. Več o krovnih vlogah je v poglavju 7.4 Krovne vloge. Krovno vlogo lahko uporabnik pridobi, tako da mu je bila v IS Monitoring dodeljena uporabniška vloga. To seveda za novega uporabnika, ki se je prijavil prvič, ni mogoče.
7. Glede na rezultat prejšnje točke (torej ugotavljanje ali ima krovno vlogo, ne glede na to, kakšna je):
- Ima krovno vlogo: Uporabnika preusmerimo v IS Monitoring in tam nadaljuje z uporabo
 - Nima krovne vloge: Uporabnika preusmerimo na stran za zahtevo za dodelitev dostopa do IS Monitoring. Več v poglavju 7.3.

7.2.2. Registracija z ročno registracijo zunanje storitve

Administrator IS Monitoring SSO ročno izdela novega uporabnika v IS Monitoring SSO, tako da ustvari novega uporabnika, vpiše zahtevane attribute (vključno z unikatnim e-poštnim naslovom), mu dodeli začasno geslo. Prijavi se v imenu tega uporabnika, zato da se skladno s točko 6.d iz prejšnjega poglavja izdela nova identiteta v evidenci uporabnikov. Nato mu geslo pobriše in s tem onemogoči prijavo uporabnika.

Znotraj IS Monitoring SSO administrator uporabniku pripravi trajen žeton, ki ga posreduje skrbniku zunanje storitve.

V IS Monitoring mu ročno dodeli ustrezne dostope (vloge in pravice).

Zunanja storitev ob klicu na podlagi trajnega žetona od IS Monitoring SSO pridobi začasen žeton (access token), s katerim izvaja klice.

Ta uporabnik ne dostopa do uporabniškega vmesnika in zato proces njegove prijave odstopa od ostalih uporabnikov.

7.2.3. Registracija z ročno registracijo uporabnika, ki uporablja uporabniško ime in geslo

Omenjen način je onemogočen na produkcijskem okolju!

Ta način je tehnično podprt na vseh okoljih, vendar je na produkcijskem okolju onemogočen. Uporaba uporabniških imen in gesel je slaba praksa in je podvržena več varnostnim tveganjem, med katerimi sta najpomembnejši:

- Slaba kvaliteta gesel in
- Posojanje uporabniških imen in gesel

Kljub mehanizmom za zmanjšanje tveganj, teh pomanjkljivosti ni mogoče odpraviti. Dodatno uporaba tega mehanizma predstavlja dodaten pritisk na koordinatorje sistema, še posebej v primeru večjega števila uporabnikov, ki hkrati redko uporabljajo sistem, kar velja tudi za IS Monitoring.

Aktivacija prijave z uporabniškim imenom in geslom je na produkcijskem okolju prepovedana!



Administrator IS Monitoring SSO ročno izdelava novega uporabnika v IS Monitoring SSO, tako da ustvari novega uporabnika, vpiše zahtevane attribute (vključno z unikatnim e-poštnim naslovom), mu dodeli začasno geslo in se prijavi v imenu tega uporabnika, zato da se, skladno s točko 6.d iz poglavja 7.2.1 Registracija z uporabo zunanje storitve SI-CAS, izdelava nova identiteta v evidenci uporabnikov. Nato geslo posreduje uporabniku.

V IS Monitoring uporabniku ročno dodeli ustrezne dostope (vloge in pravice).

Uporabnik je ob dostopu do spletnega naslova IS Monitoring preusmerjen na IS Monitoring SSO, kjer bo na voljo (poleg SI-CAS) tudi vpis uporabniškega imena in gesla. Po prijavi uporabnik nadaljuje delo v IS Monitoring.

IS Monitoring ne omejuje trajanja gesel, kompleksnosti gesel itd.

7.3. Zahtevek za dodelitev in/ali odvzem dostopa

Znotraj IS Monitoring je zahtevek za dodelitev in/ali odvzem dostopa zapis v podatkovni zbirki s podatki uporabnika, ki je zahtevo oddal, opisom zahteve, komentarjem koordinatorja in statusom zahtevka.

7.3.1. Oddaja zahtevka za dodelitev in/ali odvzem dostopa

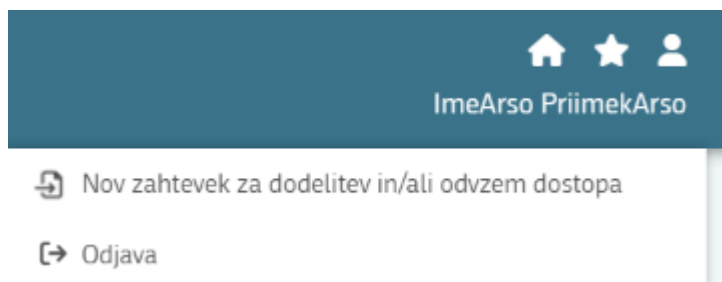
Zahtevek za dodelitev in/ali odvzem dostopa lahko odda le registriran in prijavljen uporabnik. Postopek za registracijo je impliciten in opisan v poglavju 7.2 Registracija novih uporabnikov aplikacij IS Monitoring.

Zahtevek za dodelitev in/ali odvzem dostopa je implementiran kot ločena API storitev, ki ne zahteva krovne vloge. Odda jo torej lahko vsak uporabnik IS Monitoring, tudi če že ima dostop do IS Monitoring.

Zahtevek vsebuje podatke uporabnika, ki oddaja zahtevek, to je uporabnika, ki je prijavljen. Uporabnik na zahtevku izbere organizacijo (iz seznama AJ PES) in eno ali več uporabniških vlog iz seznama. Uporabniku se ponudijo vse možne uporabniške vloge, ki so definirane (uporabniške vloge so podrobno opisane v vsebinskih analizah). Poleg tega vsebuje tudi besedilno polje, v katerega uporabnik vpiše utemeljitev zahtevka. Uporabnik lahko tudi opsijsko zahteva odvzem že dodeljenih vlog za izbrano organizacijo preko izbire že dodeljenih uporabniških vlog iz seznama. Uporabnik zahtevek odda (se shrani v aplikacijo). Za tem je preusmerjen na pregled izpolnjenega zahtevka, kjer ga natisne. PDF oblika zahtevka se uporabniku prav tako pošlje na e-poštni naslov.

Zahtevek izven konteksta IS Monitoring uporabnik posreduje odgovorni osebi za podpis. Podpisan zahtevek pošlje uporabnik ali odgovorna oseba po elektronski pošti nazaj na ARSO. ARSO preveri pravilnost zahtevka, nato odobri ali zavrne dodelitev vlog.

IS Monitoring uporabnikov ne omejuje pri številu zahtevkov in jih je mogoče kreirati tudi naknadno.



Slika 7: Gumb za oddajo novega zahtevka v aplikaciji

Po oddaji zahtevka je ta viden koordinatorjem IS Monitoring v evidenci uporabnikov. Po oddaji zahtevka podatkov ni možno spreminjati. Doda se lahko le še komentar koordinatorja in spremeni status v bodisi ODOBREN bodisi v ZAVRNJEN. V tem primeru je uporabnik obveščen avtomatsko preko elektronske pošte.

Sklop je sestavljen iz tekstovnega polja, ki vsebuje navodila za izpolnjevanje obrazca, in sklopa, ki je zasnovan kot forma in vsebuje osnovne podatke o uporabniku.

Slika 8: Stran Zahtevek za dodelitev in/ali odvzem dostopa

Sklop »Podatki zahtevka« vsebuje naslednja polja:

POLJE	MOŽNOST UREJANJA	OBVEZNOST	TIP POLJA ZA UREJANJE	OPIS
Enolični identifikator	NE	DA	/	Polje prikazuje enolični identifikator uporabnika v obliki 112345678. Polje je povezava do strani Uporabnika (Povezava je omogočena le za koordinatorje IS Monitoring).
Ime	NE	DA	/	Polje prikazuje ime uporabnika. Podatek se ob vsaki prijavi prenese iz IS Monitoring SSO.
Priimek	NE	DA	/	Polje prikazuje priimek uporabnika. Podatek se ob vsaki prijavi prenese iz IS Monitoring SSO.
E-pošta	NE	DA	/	Polje prikazuje e-pošto uporabnika. Podatek se ob vsaki prijavi prenese iz IS Monitoring SSO.



Telefon	DA	NE	Vnosno polje	Polje prikazuje telefonsko številko uporabnika.
Organizacija	DA	DA	Spustni seznam	S klikom na polje se odpre spustni seznam organizacij (AJPES).
Uporabniška vloga za dodelitev	DA	NE (pogojno)	Spustni seznam	S klikom na polje se odpre spustni seznam uporabniških vlog za katere uporabnik zahteva dostop. Uporabnik izbere eno ali več vlog. Obvezno mora biti izpolnjeno vsaj eno od polj za Uporabniško vlogo (za dodelitev ali odvzem).
Uporabniška vloga za odvzem	DA	NE (pogojno)	Spustni seznam	S klikom na polje se odpre spustni seznam uporabniških vlog za katere uporabnik zahteva odvzem. Uporabnik izbere eno ali več vlog. Seznam je omejen na uporabniške vloge, ki jih ima uporabnik trenutno dodeljene pri izbrani organizaciji. Obvezno mora biti izpolnjeno vsaj eno od polj za Uporabniško vlogo (za dodelitev ali odvzem).
Utemeljitev	DA	NE	Vnosno polje	V polje lahko uporabnik zapiše utemeljitev zahtevka

7.3.2. Pooblašcanje na nivoju kompleksov

Pooblašcanje na nivoju kompleksov ni del zahtevka za dodelitev dostopa, vendar se določa v evidenci kompleksov. Več v dokumentu [223925 - Analiza in načrt IS - Evidence in šifranti \(0.97\).docx](#)

7.4. Krovne vloge

V IS Monitoring bodo implementirane različne uporabniške vloge, ki pokrivajo vsebinska področja, tako kakor je funkcionalno najbolj smiselno. Uporabniške vloge so v resnici predvsem zbirka manjših pravic, kakor so določene v funkcionalnih specifikacijah. Teh vlog je veliko in se lahko skozi verzije tudi spreminjajo (ustvarjajo nove, stare se delijo itd).

S stališča varovanja sistema je ključno, da je odločitev, ali uporabnik sme ali ne sme dostopati do IS Monitoring enostavna in hitra. Tudi zato, ker je to odločitev potrebno zapisati v dostopovni žeton uporabnika, ki se prenaša na strežnik z vsakim klicem. Zato identificiramo nekaj krovnih vlog, ki se skozi delovanje sistema ne spreminjajo in jih ni mogoče dodeliti uporabnikom, ampak se izračunajo na podlagi konkretnih pravic uporabnika, kakor jih dodeli koordinator IS Monitoring.

Pri tem se krovne vloge izračunajo ob vsaki spremembi pravic. Predvidene krovne vloge so:

- KV_ARSO_KOORDINATOR (le s to vlogo je mogoče dostopati do upravljanja z uporabniki)
- KV_ARSO_OBRATOVALNI_MONITORING
- KV_ARSO_DRZAVNI_MONITORING
- KV_ARSO_SIFRANTI

Pod temi krovnimi vlogami je večje število uporabniških vlog, ki pokrivajo posamezne funkcionalne sklope in so izven konteksta tega poglavja. Uporabniške vloge bodo bolj podrobno opisane v vsebinskih analizah.

7.5. Profili (Organizacije) uporabnikov

Vsak uporabnik ima različen nabor pravic, ki je odvisen od organizacije, v imenu katere deluje. V večini primerov je pričakovano, da uporabnik deluje v imenu ene organizacije. Podprto bo tudi, da v nekem trenutku uporabnik zamenja službo in se s tem pravice nad staro organizacijo deaktivirajo ter dodelijo nove za novo organizacijo. Deaktivacijo pravic uredijo koordinatorji IS Monitoring, ko



organizacija to zahteva preko elektronske pošte. Dodeljevanje pravic za novo organizacijo poteka enako kot pri prvi dodelitvi (več v poglavju 7.3). Prav tako je podprt primer, ko uporabnik deluje v več organizacijah hkrati.

Znotraj IS Monitoring je podprtih več organizacij (profilov) za enega uporabnika, uporabnik znotraj posamezne organizacije ima lahko dodeljene različne uporabniške vloge. Preklapljanje med organizacijami, nad katerimi ima uporabnik aktiven dostop, bo omogočeno preko uporabniškega vmesnika. Aktiven dostop nad organizacijo pomeni, da ima uporabnik za to organizacijo aktiven zapis in da ima za to organizacijo vsaj eno aktivno uporabniško vlogo. Nad katerimi organizacijami ima uporabnik dostop lahko koordinatorji pregledajo na sklopih, opisanih v poglavjih 7.6.2.3 in 7.6.2.3.1.

Ne glede na vrsto implementacije, je vsak profil vezan na natanko eno identiteto (uporabnika), to je zapis, ki ima enolični identifikator v obliki I12345678.

Na straneh za upravljanje z dostopi uporabnikov so prikazani osnovni podatki uporabnika, njegove organizacije in uporabniške vloge vezane na organizacijo. Dostopi (pravice) niso nikoli vezane neposredno na uporabnika, temveč vedno na organizacijo.

V strežniških dnevnikih, zgodovinskih zapisih in drugih tehničnih zapisih se vedno vodi identifikator uporabnika.

7.6. Administracija uporabnikov

V IS monitoring bo možen pregled nad registriranimi uporabniki. Do strani bo omejen dostop na uporabnike s krovno vlogo KV_ARSO_KOORDINATOR.

7.6.1. Stran seznam uporabnikov

Segment bo prikazoval seznam vseh registriranih uporabnikov v aplikaciji.

Enolični identifikator IT	Ime IT	Priimek IT	Email IT	Aktiven IT	Organizacije (uporabniške vloge) IT
I12345678	Janez	Novak	janez.novak@gor.si	Da	Gorenje d.o.o. (Upravljevec)
I12345679	Peter	Lin	peter.lin@krka.si	Da	Krka, d.d. (Upravljevec)
I12345680	Ana	Novak	ana.novak@tes.si	Da	Termoelektrarna Soštanj (TES) (Upravljevec)
I12345681	Maja	Kovac	maja.kovac@nek.si	Da	Nuklearna elektrarna Krško (NEK) (Upravljevec)
I12345682	Luka	Zupan	luka.zupan@ob.si	Da	Odlagališče Barje (Upravljevec)
I12345683	Nina	Potočnik	nina.potocnik@ccn.si	Da	Centralna čistilna naprava (CCN) Ljubljana (Upravljevec)
I12345684	Sara	Kralj	sara.kralj@pp.si	Da	Perutnina Ptuj d.d. (Upravljevec)
I12345685	Matej	Vidmar	matej.vidmar@kf.si	Da	Kemofarmacija d.d. (Upravljevec)
I12345686	Petra	Kos	petra.kos@nlzoh.si	Da	NLZOH (izvajalec DM)

Slika 9: Seznam uporabnikov

V tabeli bodo naslednji stolpci:

POLJE	OPIS
Enolični identifikator	Polje prikazuje enolični identifikator uporabnika v obliki I12345678 Polje je povezava do podrobnosti uporabnika (več v naslednjem poglavju).



Ime	Polje prikazuje ime uporabnika.
Priimek	Polje prikazuje priimek uporabnika.
E-pošta	Polje prikazuje e-pošto uporabnika.
Aktiven	Polje določa ali je uporabnik aktiven.
Organizacije (uporabniške vloge)	Polje vsebuje podatek, katerim organizacijam pripada uporabnik ter v oklepaju pripisan podatek o dodeljenih uporabniških vlogah na tej organizaciji.

Kriteriji nad seznamom uporabnikov

Seznam uporabnikov za omejevanje prikazanih rezultatov vsebuje kriterije, s katerimi se lahko omejujemo po prikazanih rezultatih in sicer:

KRITERIJ	TIP KRITERIJA	OBVEZEN	FUNKCIONALNOST
Vsebuje podatek	Iskalni niz	NE	Omogoča prosti vpis teksta in iskanje po delih besede po vseh stolpcih tabele.
Enolični identifikator	Vpisno polje	NE	Možnost vpisa in iskanje po enoličnem identifikatorju.
Ime	Vpisno polje	NE	Možnost vpisa in iskanje po imenu.
Priimek	Vpisno polje	NE	Možnost vpisa in iskanje po priimku.
Aktiven	Izbirno polje	NE	Možnost izbire iskanja po aktivnih ali neaktivnih uporabnikih.
Organizacija	Izbirno polje	NE	S klikom na polje se odpre spustni seznam organizacij (AJ PES).
Uporabniška vloga	Izbirno polje	NE	S klikom na polje se odpre spustni seznam uporabniških vlog.
Status zahtevka	Izbirno polje	NE	S klikom na polje se odpre spustni seznam statusov zahtevkov za dostop.

7.6.2. Stran Uporabnik

Stran »Uporabnik« bo vsebovala:

- osnovne podatke o uporabniku,
- uporabnikove certifikate za prijavo,
- organizacije, katerim uporabnik pripada in njegovo tamkajšnjo vlogo
- uporabnikove zahteve za dodelitev dostopa.

Slika 10: Stran Uporabnik



7.6.2.1. Sklop Osnovi podatki

Sklop bo prikazoval osnovne podatke uporabnika. Zasnovan bo kot sklop s polji. Urejati bo možno le določena polja.

Osnovni podatki				Uredi
Enolični identifikator I12345678	Ime Janez	Priimek Novak	Email janez.novak@gor.si	
Telefon 01 123 456	Aktiven Da	Datum kreiranja 01.01.2024	Datum zadnje spremembe 06.05.2024	
Datum zadnje prijave 28.10.2024	Datum zadnje spremembe pravic 28.10.2024	SI-CAS ID 0101900500000		

Slika 11: Sklop Osnovni podatki na strani Uporabnik

Sklop bo vseboval naslednje podatke:

POLJE	MOŽNOST UREJANJA	OBVEZNOST	TIP POLJA ZA UREJANJE	OPIS
Enolični identifikator	NE	DA	/	Polje prikazuje enolični identifikator uporabnika v obliki I12345678
Ime	NE	DA	/	Polje prikazuje ime uporabnika. Podatek se ob vsaki prijavi prenese iz IS Monitoring SSO.
Priimek	NE	DA	/	Polje prikazuje priimek uporabnika. Podatek se ob vsaki prijavi prenese iz IS Monitoring SSO.
E-pošta	NE	DA	/	Polje prikazuje e-pošto uporabnika. Podatek se ob vsaki prijavi prenese iz IS Monitoring SSO.
Telefon	DA	NE	Vnosno polje	Polje prikazuje telefonsko številko uporabnika.
Aktiven	DA	DA	Spustni seznam	Izbira vrednosti Da ali Ne. Polje določa ali je uporabnik aktiven. V primeru, da je uporabnik neaktiven izgubi dostop na vse strani z omejenim dostopom (še vedno lahko dostopa do strani za oddajo zahtevkov za dostop).
Datum kreiranja	NE	DA	/	Polje prikazuje datum in čas, ko se je uporabniški račun kreiral.
Datum zadnje spremembe	NE	DA	/	Polje prikazuje zadnji datum in čas, ko so se podatki o uporabniku spremenili. Nekatere podatke posodablja sam IS Monitoring SSO.
Datum zadnje prijave	NE	DA	/	Polje prikazuje datum in čas, ko se je uporabnik nazadnje prijavil.
Datum zadnje spremembe pravic	NE	DA	/	Polje prikazuje datum in čas, ko so se uporabniku spremenile pravice.
SI-CAS ID	NE	DA	/	Polje prikazuje enolični identifikator iz SI-CAS.

7.6.2.2. Sklop Uporabnikovi certifikati

Sklop bo prikazoval podatke certifikatov uporabnika s katerimi se je prijavil v aplikacijo preko SI-CAS. Podatkov ne bo možno urejati.



Uporabnikovi certifikati				
Javni ključ certifikata	Izdajatelj certifikata	Veljaven od	Veljaven do	Zadnja prijava
a1a32b6a4401d1b72f0531e4efc9611d1fa028c08be3c373b6788e022abbf132	Ministrstvo za javno upravo	1.1.2020	1.1.2030	28.10.2024
Prikazanih: 1 od 1				
<div> <div>1</div> <div>10</div> </div>				
<div>Uredi</div>				
Javni ključ certifikata a1a32b6a4401d1b72f0531e4efc9611d1fa028c08be3c373b6788e022abbf132		Izdajatelj certifikata Ministrstvo za javno upravo		
Veljaven od	Veljaven do	Zadnja prijava		
1.1.2020	1.1.2030	28.10.2024		

Slika 12: Sklop Uporabnikovi certifikati na strani Uporabnik

Na segmentu je tabela z naslednjimi stolpci:

POLJE	OPIS
Javni ključ certifikata	Polje prikazuje javni ključ certifikata.
Izdajatelj certifikata	Polje prikazuje podatke o izdajatelju certifikata.
Veljaven od	Polje prikazuje začetek veljavnosti certifikata.
Veljaven do	Polje prikazuje konec veljavnosti certifikata.
Zadnja prijava	Polje prikazuje čas ko se je uporabnik nazadnje prijavil s tem certifikatom.

7.6.2.3. Sklop Organizacije

Sklop bo prikazoval katerim organizacijam pripada uporabnik. Urejati bo možno le določena polja. Omogočeno bo dodajanje zapisov. Samo pri dodajanju novega zapisa bo omogočena izbira organizacije. Branje zapisov bo onemogočeno. Zapisa se lahko deaktivira.

Organizacije

Išči po tabeli...

Uredi

Organizacija	Aktiven od	Aktiven do	Aktiven
Gorenje d.o.o.	16.10.2021	16.10.2031	Da

Prikazanih: 1 od 1

1

10

Uporabniške vloge

Išči po tabeli...

Uredi

Uporabniška vloga	Opis uporabniške vloge
Gorenje d.o.o.	Upravljevec kompleksa

Prikazanih: 1 od 1

1

10

Slika 13: Sklop Organizacije na strani Uporabnik

Na segmentu je tabela z naslednjimi stolpci:

POLJE	MOŽNOST UREJANJA	OBVEZNOST	TIP POLJA ZA UREJANJE	OPIS
Organizacija	DA (samo pri dodajanju)	DA	Spustni seznam	S klikom na polje se odpre spustni seznam organizacij (AJPES).



Aktiven od	DA	DA	Datum	Polje omogoča vnos ali izbiro datuma začetka aktivnosti pripadnosti organizaciji.
Aktiven do	DA	NE	Datum	Polje omogoča vnos ali izbiro datuma konca aktivnosti pripadnosti organizaciji.
Aktiven	NE	DA	/	Polje prikazuje ali je zapis aktiven glede na polji Aktiven od in Aktiven do.

7.6.2.3.1 Podsklop Uporabniške vloge

Podsklop Uporabniške vloge prikazuje seznam uporabniških vlog. Zasnovan bo kot tabela, ki bo podrejena tabeli z organizacijami preko katere bo uporabniku omogočeno dodajati in odstranjevati uporabniške vloge. Odstranjevanje in dodajanje je omogočeno, ko je tabela v načinu urejanja s klikom na gumb »Uredi«. Urejanje dodanih vlog ni omogočeno.

Pri izbiri organizacije v zgornji tabeli se pokaže seznam vseh dodeljenih uporabniških vlog za organizacijo.

Uporabniška vloga	Opis uporabniške vloge
Gorenje d.o.o.	Upravljaec kompleksa

Slika 14: Podsklop Uporabniške vloge na strani Uporabnik

Na segmentu je tabela z naslednjimi stolpci:

POLJE	MOŽNOST UREJANJA	OBVEZNOST	TIP POLJA ZA UREJANJE	OPIS
Uporabniška vloga	NE	DA	Spustni seznam	Polje prikazuje naziv uporabniške vloge.
Uporabniška vloga (opis)	NE	DA	/	Polje prikazuje opis uporabniške vloge.

7.6.2.4. Sklop Zahtevki za dodelitev dostopa

Sklop bo prikazoval podatke Zahtevkov za dodelitev dostopa, ki jih je oddal uporabnik. Podatkov ne bo možno urejati.



Zahtevki za dodelitev dostopa

Išči po tabeli...

Uredi

Številka zahtevka <div></div>	Status zahtevka <div></div>	Datum oddaje zahtevka <div></div>
61239	ODDAN	24.8.2024

Prikazanih: 1 od 1

1

10

Uredi

Številka zahtevka

61239

Datum oddaje zahtevka

24.8.2024

Organizacija

Gorenje d.o.o.

Uporabniška vloga za dodelitev

Upravitelj

Uporabniška vloga za odvzem

-

Utemeljitev

-

Status zahtevka

ODDAN

Komentar koordinatorja

-

Slika 15: Sklop Zahtevki za dodelitev dostopa na strani Uporabnik

Na segmentu je tabela z naslednjimi stolpci:

POLJE	MOŽNOST UREJANJA	OBVEZNOST	TIP POLJA ZA UREJANJE	OPIS
Številka zahtevka	NE	DA	Spustni seznam	Polje prikazuje številko zahtevka. Polje je povezava do strani Zahtevek za dodelitev dostopa.
Status zahtevka	DA	DA	Spustni seznam	Polje prikazuje v katerem statusu je zahtevek. (ODDAN, ZAVRNJEN, ODOBREN)
Datum oddaje zahtevka	NE	DA	/	Polje prikazuje, kdaj je bil zahtevek oddan (shranjen v aplikacijo).

S klikom na zapis se prikaže podroben prikaz oddanega zahtevka. Izbran zahtevek je mogoče urediti, če ni v statusu "ODOBREN" ali "ZAVRNJEN".

Zapis za podroben prikaz je zasnovan kot forma z naslednjimi podatki:

POLJE	MOŽNOST UREJANJA	OBVEZNOST	TIP POLJA ZA UREJANJE	OPIS
Številka zahtevka	NE	DA	Spustni seznam	Polje prikazuje številko zahtevka. Polje je povezava do strani Zahtevek za dodelitev dostopa.
Status zahtevka	DA	DA	Spustni seznam	Polje prikazuje v katerem statusu je zahtevek. (ODDAN, ZAVRNJEN, ODOBREN)
Datum oddaje zahtevka	NE	DA	Datum	Polje prikazuje, kdaj je bil zahtevek oddan (shranjen v aplikacijo).
Datum obravnave zahtevka	NE	DA	Datum	Polje prikazuje, kdaj se je zahtevku spremenil status v ZAVRNJEN ali ODOBREN.
Komentar koordinatorja	DA	DA	Vnosno polje	Polje prikazuje komentar, ki ga je koordinator podal na zahtevek.
Organizacija	NE	DA	Spustni seznam	Polje prikazuje organizacijo uporabnika.
Uporabniška vloga za dodelitev	NE	NE	Spustni seznam	Polje prikazuje seznam uporabniških vlog za katere uporabnik zahteva dostop.
Uporabniška vloga za odvzem	NE	NE	Spustni seznam	Polje prikazuje seznam uporabniških vlog za katere uporabnik zahteva odvzem dostopa.



Utemeljitev	NE	NE	Vnosno polje	Polje prikazuje utemeljitev zahtevka.
-------------	----	----	--------------	---------------------------------------