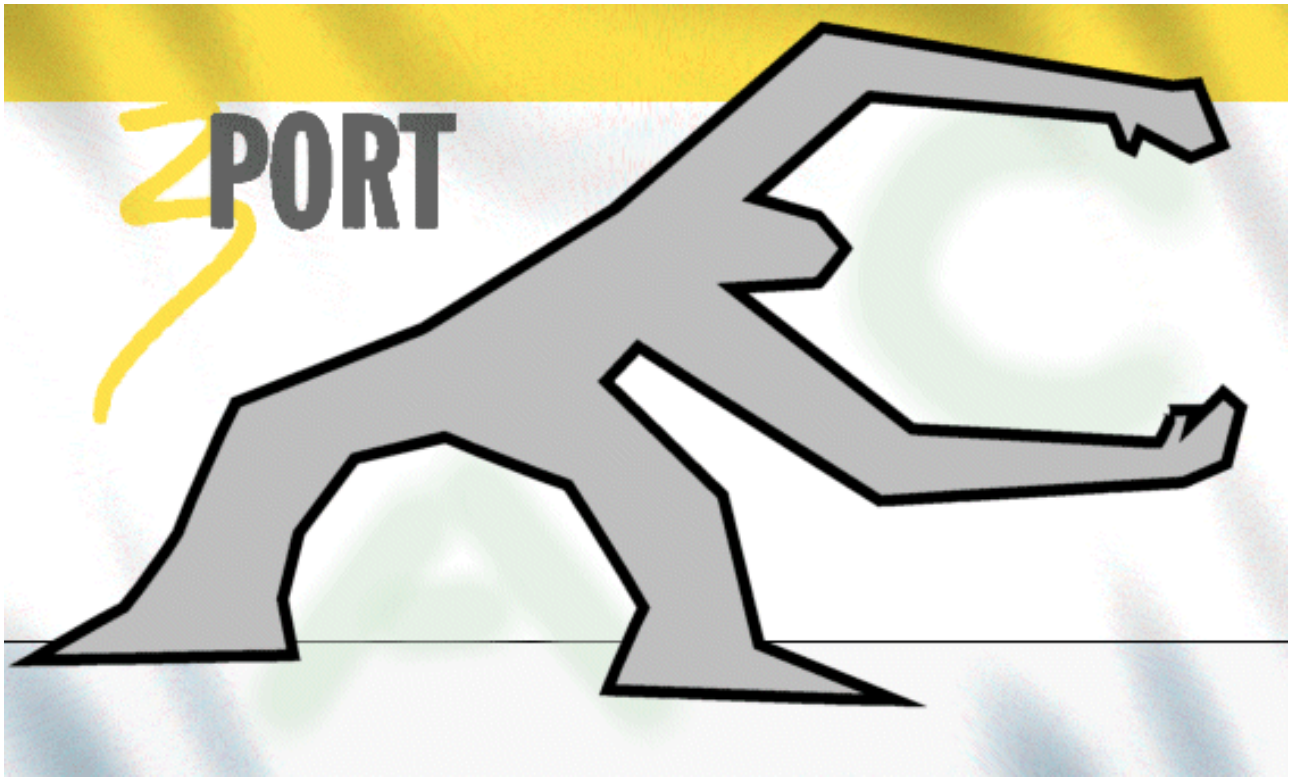
ADAM (1.27)

Administriranje uporabniških pravic za aplikacije v spletnem operacijskem okolju 3iOS



Kazalo vsebine

1. Kaj je Adam?....3
2. Kaj določamo z ADAM-om?....3
   2.1 Vrste uporabnikov (uporabniških računov)....3
   2.2 Vloge (ang.: "Role")....3
   2.3 Področja dela/uradi/oddelki/....4
   2.4 Delovna mesta (za področje dela/v uradu/v oddelku)....4
   2.5 Uporabniki....4
   2.6 Pristopna gesla....5
   2.7 Upravljanje uporabniških dovoljenj nad aplikacijami....5
   2.8 Dodeljevanje in upravljanje z ACL listami (Access Control List)....5
   2.9 Brisanje uporabniških računov....8
3. ADAM in uporabniški vmesnik....8
4. ADAM in revizijske sledi....10

Zgodovina različic:

Različica	Datum	Sprememba
1.0	26. 08. 2014	Prva izdaja navodila
2.0	21. 12. 2016	Revizija za ETZ
3.0	16. 03. 2018	Dodana tč. d) v poglavje 3 ADAM in uporabniški vmesnik zaradi nove funkcionalnosti: časovna omejitev dostopa do posameznih možnosti oz. funkcij (do datuma ali po datumu)

1. Kaj je Adam?

Vse spletne aplikacije in zaledne storitve podjetja 3 PORT, se izvajajo v našem spletnem operacijskem okolju 3iOS (*"3 PORT-ov internetni operacijski sistem"*).

ADAM je skupina krmilnih tabel za centralno upravljanje uporabniških dostopov in določanje nivojev pravic za delo s posameznimi spletnimi aplikacijami znotraj sistema 3iOS in z dokumenti znotraj posameznih aplikacij.

Parametre v krmilnih tabelah na bazi nastavlja izvajalec (**Sistemski administrator**), glede na zahteve in potrebe naročnika.

Za nastavljanje tistih krmilnih parametrov, ki jih lahko izvaja tudi pooblaščeni administrator na strani naročnika (**Uporabniški administrator**) pa je nad sistemom tabel ADAM zgrajen grafični vmesnik.

Grafični vmesnik lahko živi v okolju 3iOS kot samostojna aplikacija, najpogosteje pa je kar integriran v dokumentni sistem VOPI.

Kdo bo dostopal (UserAdmin) do grafičnega vmesnika in kako bo ta integriran določimo tudi z ADAM-om.

2. Kaj določamo z ADAM-om?

2.1 Vrste uporabnikov (uporabniških računov)

V ADAM-u ločimo tri vrste uporabnikov (uporabniških računov):

- **admin** --> je sistemski administrator, ki ima najvišja (vsa) pooblastila nad sistemom, nima pa vpogleda v dokumente v sistemu. Rola sistemskega administratorja je v domeni izvajalca 3 PORT.
- **system_user** --> je sistemski uporabnik, ki se uporablja za sistemsko zaledno obdelavo podatkov ali za občasna izjemna ali masovna dela, ki bi bila prezahtevna ali predolgotrajna, da bi jih uporabniki izvedli po standardnem podprtem postopku preko aplikacije. Rola sistemskega uporabnika je v domeni izvajalca 3 PORT.
- **user**-->je uporabnik aplikacije. Vse role in različni nivoji pooblastil se določajo na nivoju posameznega uporabnika aplikacije (npr. "Uporabniški administrator") ali posameznih skupin uporabnikov aplikacije (npr. "uslužbenci v uradu", "uslužbenci v oddelku A", "delavci v glavni pisarni", ipd.)

2.2 Vloge (ang.: "Role")

Ločimo:

1. "**Aplikativne vloge**" – so različne funkcije, ki so programsko podprte v posamezni aplikaciji in jih lahko vsako posebej aktiviramo ali de-aktiviramo in to lahko dela tudi uporabnik z ustrezno rolo

2. "**Uporabniške vloge**" – so ena ali več aplikativnih vlog združenih v eno funkcionalno celoto oz. skupino, ki ustreza določenemu "delovnemu mestu". Skupine so lahko gnezdene v poljubno mnogo vozlišč.
3. "**Sistemske vloge**" - nastavljamo jih kot ponudnik sistema za pravilno delovanje sistema (npr. Rola za dodeljevanje rol) in niso na voljo uporabnikom sistema

Aplikativne vloge so določene za vsako aplikacijo posebej in se implementirajo že v fazi razvoja. Pri razvoju aplikacije za 3iOS projektant IS predpiše posamezne vloge, ki jih mora aplikacija podpirati glede na računalniško podporo procesom in vsebino dela z aplikacijo.

Sistemski administrator za vsako novo aplikacijo vpiše aplikativne vloge v krmilno tabelo sistema ADAM. Prav tako lahko več aplikativnih vlog združuje v skupine oz. "Uporabniške vloge". Te vloge se lahko drevesno vejajo v poljubno globino podskupin glede skupne lastnosti (npr. VOPI/Glavna pisarna, VOPI/Referenti).

Uporabniški administrator lahko posameznemu uporabniku aplikacije vklopi ali izklopi poljubne uporabniške vloge. Pri tem posameznih aplikativnih vlog znotraj uporabniške skupine ne more spreminjati.

Seznam vseh podprtih vlog je dostopen

– 1 in 2 v drevesu spletne aplikacije
– 1, 2 in 3 v razvojnem Wikiju.

2.3 Področja dela/uradi/oddelki/

Področje dela tu imenujemo "Urad". Določa jih **Uporabniški administrator,** skladno s signirnim načrtom organizacije.

Za vsako področje/urad/oddelek se avtomatično tvori tudi predstojnik ter tajništvo.

2.4 Delovna mesta (za področje dela/v uradu/v oddelku)

Delovna mesta tu imenujemo "Job". Znotraj področja/urada/oddelka jih določa uporabnik aplikacije s pooblastilom **Uporabniški administrator** skladno s signirnim načrtom.

2.5 Uporabniki

Uporabnike tu imenujemo tudi "User". Določa jih uporabnik aplikacije s pooblastilom **Uporabniški administrator.**

Vsak uporabnik je lahko aktiven ali neaktiven (logično brisan).

Obvezen podatek uporabnika je e-poštni naslov zaradi samodejnega dodeljevanja prijavnega gesla v sistem 3iOS, ...).

Uporabniški administrator uporabniku določi tudi:

- katero delovno mesto zaseda, skladno s signirnim načrtom ("**user-job**").
- dovoljenja za delo z aplikacijami ("**role**")
- dovoljenja za delo z dokumenti ("**ACL liste**")

2.6 Pristopna gesla

Gesla avtomatično določa ADAM in so ostalim uporabnikom nedostopna. Postopek določitve gesla sproži uporabnik ob prvi prijavi z akcijo v 3iOS-u "**Pozabil sem geslo**"

Z vpisom e-pošte ADAM izvede kontrolo na obstoj uporabnika v ADAM-u. Če je v ADAM-u določen uporabnik ali več uporabnikov z vpisanim e-naslovom, bo na navedeni naslov poslal e-pošto z navedenimi vsemi uporabniškimi imeni, gesli in uradi.

Če vpiše naslov, ki ni določen pri nobenem uporabniku, bo uporabnik dobil obvestilo, da uporabnik ne obstaja. V tem primeru se mora obrniti na Uporabniškega administratorja, da ga najprej evidentira v ADAM-a. .

Če vpiše tuj naslov, ki obstaja v ADAM-u, bo drugemu uporabniku resetiral geslo in ta bo tudi prejel obvestilo o novem geslu. ADAM beleži IP iz katerega je bil zahtevek poslan.

2.7 Upravljanje uporabniških dovoljenj nad aplikacijami

- upravljanje dovoljenj na nivoju uporabnika (aktiven/neaktiven, kdo ima dovoljenje proženja sistemskih funkcij)
- upravljanje dovoljenj na nivoju aplikacij
- upravljanje dovoljenj na nivoju dokumentov/zadev (glej ACL-je)
- upravljanje dovoljenj na nivoju oddelkov (vsi uporabniki na oddelku podedujejo ta dovoljenja)
- združevanje posameznih dovoljenj v posamezne role (rola GLPI ima VOPI/GLPI, VIP/GLPI in VVP/GLPI)

2.8 Dodeljevanje in upravljanje z ACL listami (Access Control List)

Dodeljevanje pravic se izvaja z *Access Control Listami (ACL).*

ACL lista je struktura, s katero sistemski administrator predpiše pravice dostopa do dokumenta ali skupine dokumentov za uporabnike na določenem delovnem mestu oz. za uporabnike iz urada.

ACL lista se lahko nanaša na uporabnika, stanje dokumenta ali zadeve, določeni deli načrta razvrščanja gradiva, oddelek, skupino uporabnikov.

Privzeto je, da noben uporabnik nima pravic dostopa. Z ACL listo se pravice dodeljujejo in sicer:

- dodelitev dostopa do določenih zadev ali dokumentov;
- dodelitev dostopa do določenih razredov načrta razvrščanja gradiva;
- dodelitev dostopa skladno z varnostnim dovoljenjem uporabnika (kadar je smiselno);
- dodelitev dostopa do posameznih možnosti in funkcij (npr. branja, posodabljanja oz. uničenja določenih elementov metapodatkov) – to lahko izvaja uporabniški administrator preko vmesnika (glej poglavje 3 - ADAM in uporabniški vmesnik);

Seznam tipov ACL-jev	
NAME	**DESCRIPTION**
allowed	Določa vrednost dovoljenega dostopa
maxAllowed	Določa maksimalno vrednost dovoljenega dostopa (if allowed > maxAllowed then maxAllowed)

Legenda uporabljenih Entity-jev	
NAME	**DESCRIPTION**
Company.main	Root element v drevesu organizacijske sheme (ACL-ji na tem nivoju veljajo za vse uporabnike v shemi)
[creator]	Izdelovalec dokumenta
[dist.main]	Entiteta v vlogi GLPI
[odgovoren]	Trenutni nosilec edit pravice
[pošiljatelj]	Predhodni odgovoren
[prejemnik]	Naslednji odgovoren
[any]	Obstoječe entitete na dokumentu

Legenda vrednosti ACL-jev			
VALUE	**MODE**	**MAPA**	**DOKUMENT**
11	VIEW	Atributni podatki mape (brez seznamov)	n/a
12	VIEW	+ seznami (stranke, parcele, dokumenti) sumarno	n/a
13	VIEW	+ seznami detaljno (brez slik dokumentov)	Atributni podatki dokumenta (brez slike)
14	VIEW	+ slike dokumentov	+ slika dokumenta
21	EDIT	Phase	Phase
22	EDIT	+ atributni podatki + slika dokumenta + dodajanje ACL-jev	+ atributni podatki + slika + dodajanje ACL-jev

Legenda uporabljenih Rol	
NAME	**DESCRIPTION**
leader.main	Rola uporabnikov v vodstvu organizacije (župan, direktor, ...)
VPP.view_all_documents	Celoten vpogled v vse dokumente v sistemu VPP

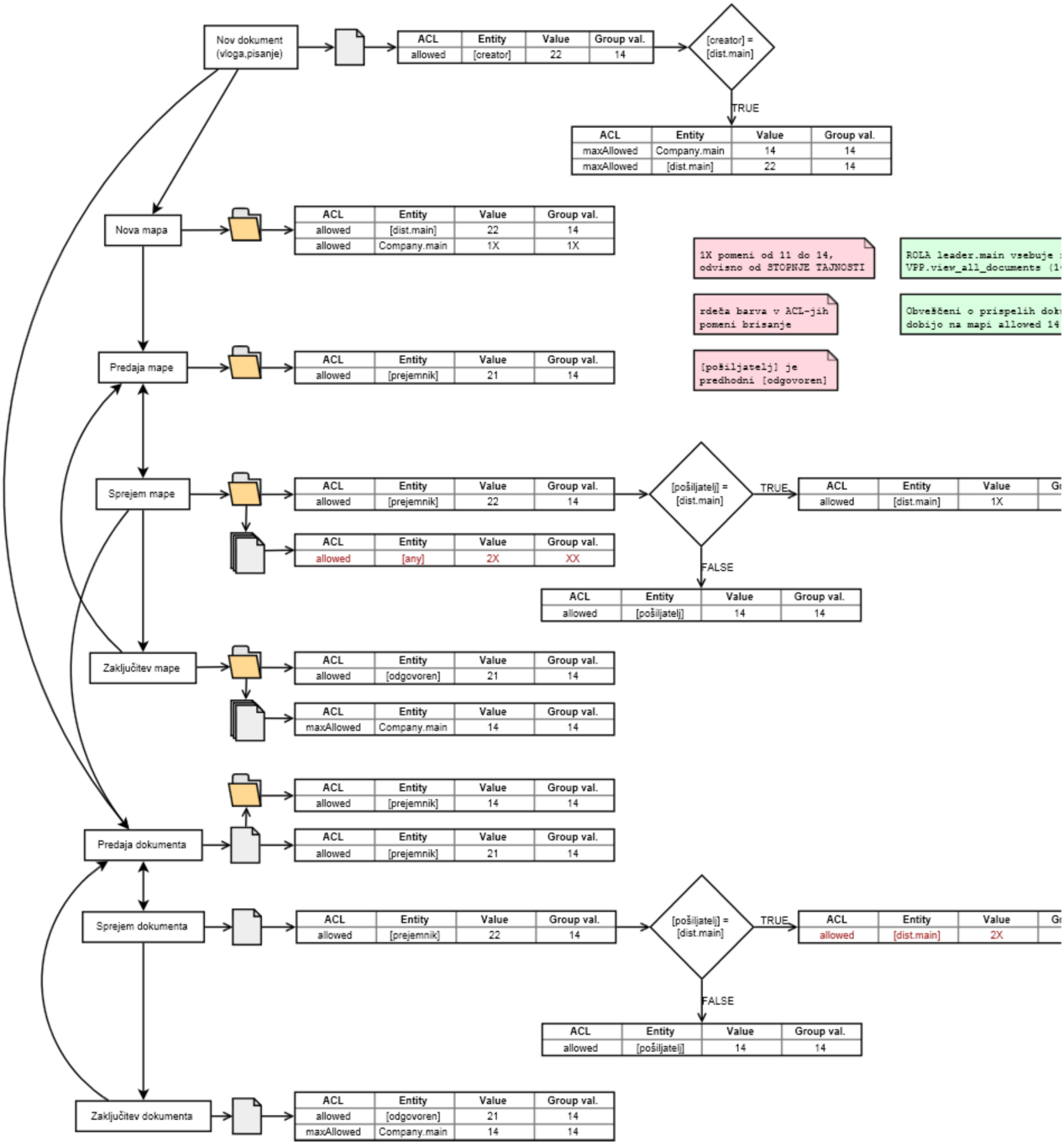


Diagram 1: Diagram nastavljanja ACL-jev

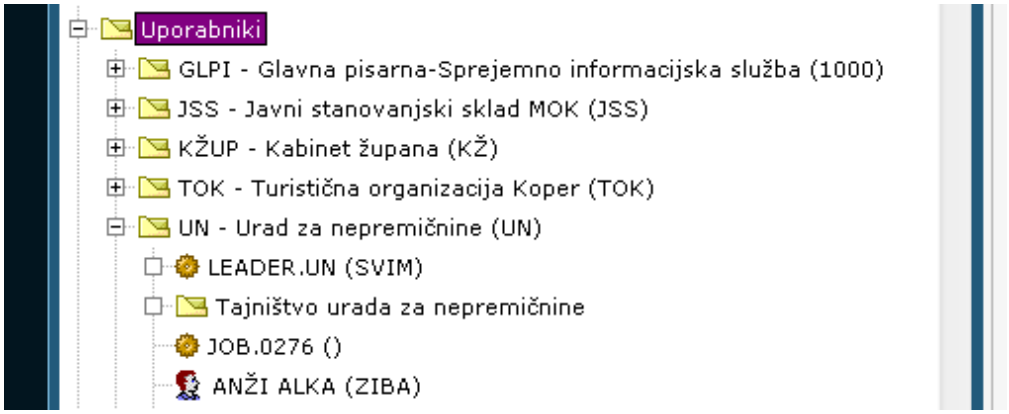
2.9 Brisanje uporabniških računov

Poteka v dveh korakih:

- brisanje uporabnika
- brisanje delovnega mesta

3. ADAM in uporabniški vmesnik

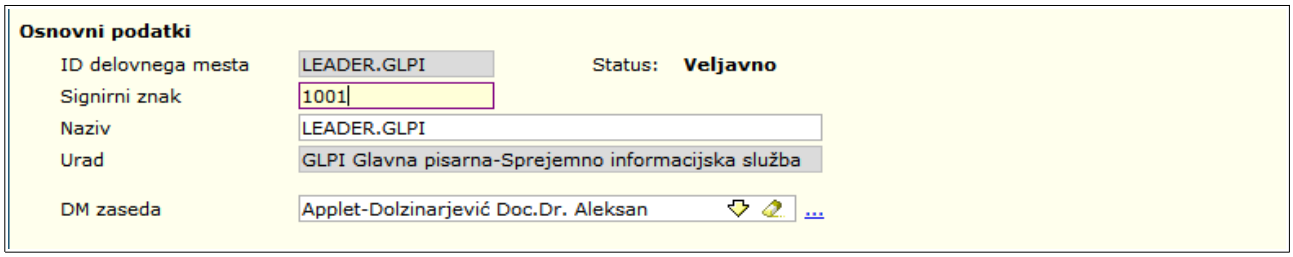
Nekatere funkcionalnosti ADAMa so dostopne tudi preko uporabniškega vmesnika, ki je vgrajen v drevo objektov aplikacije VOPI z imenom vozlišča "Uporabniki":



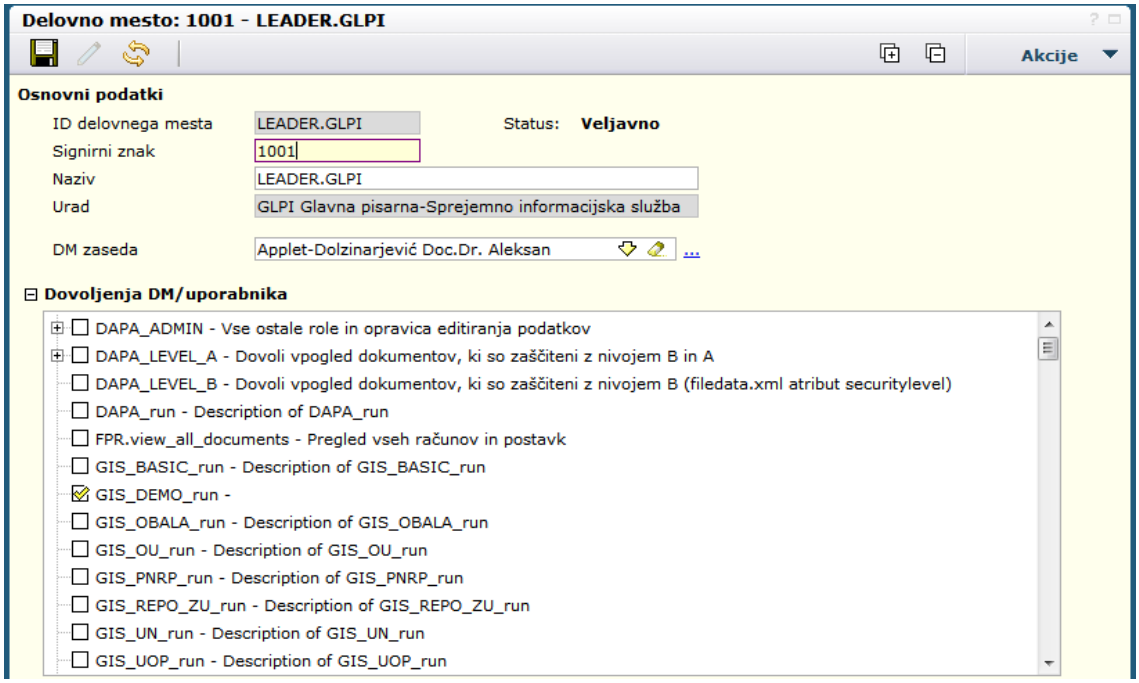
Vmesnik je namenjen vsem uporabnikom za pregledovanje uporabnikov in delovnih mest (signirni znakov). Pooblastila za urejanje podatkov se dodelijo preko ADAM-a osebi, ki je imenovana za uporabniškega administratorja. Največkrat je to uporabnik s pooblastili VOPI/GLPI - Vodja glavne pisarne.

Uporabniški administrator lahko preko vmesnika izvaja naslednje akcije:

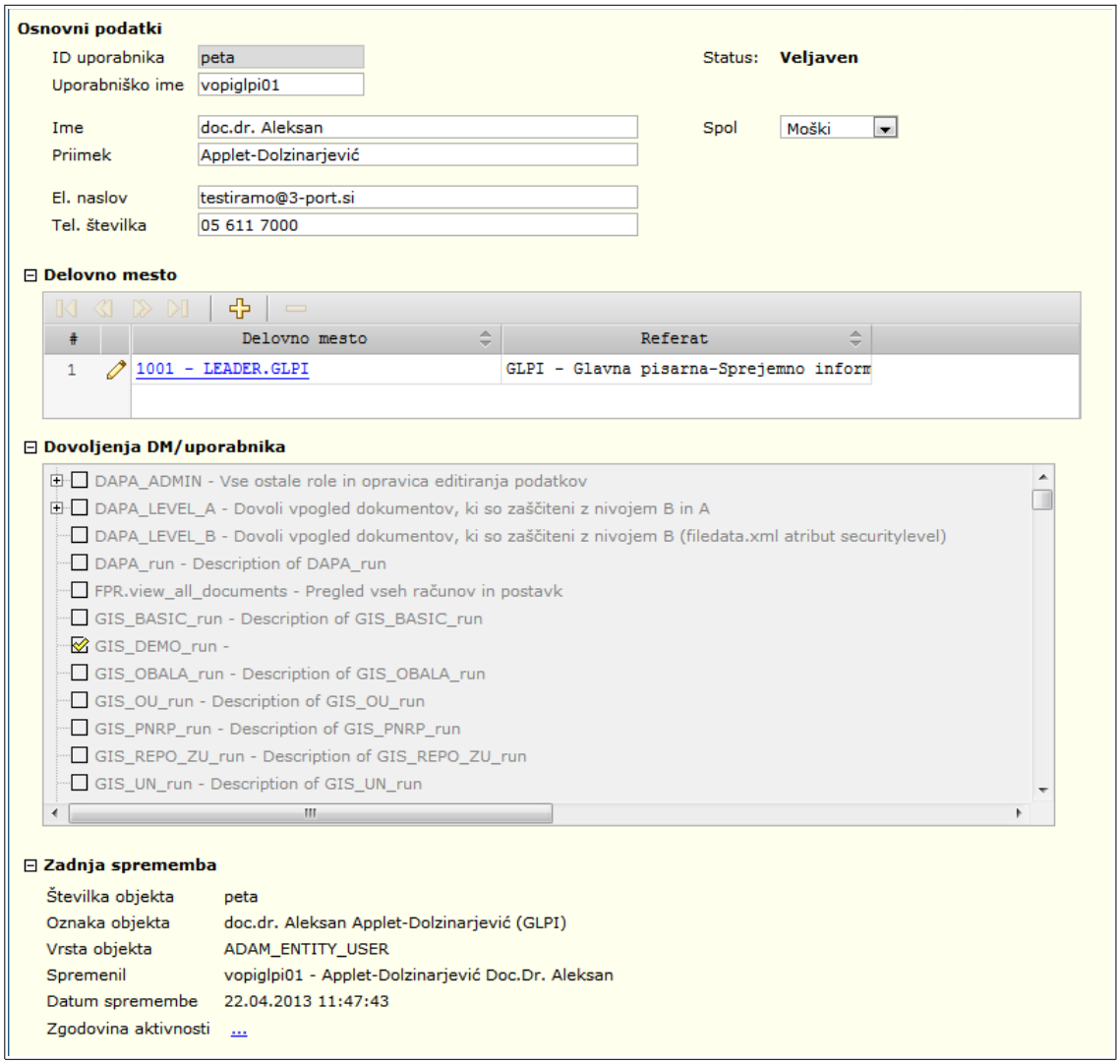
a) nastavljanje osnovnih podatkov (delovno mesto – signirni znak ter oseba, ki zaseda to DM):



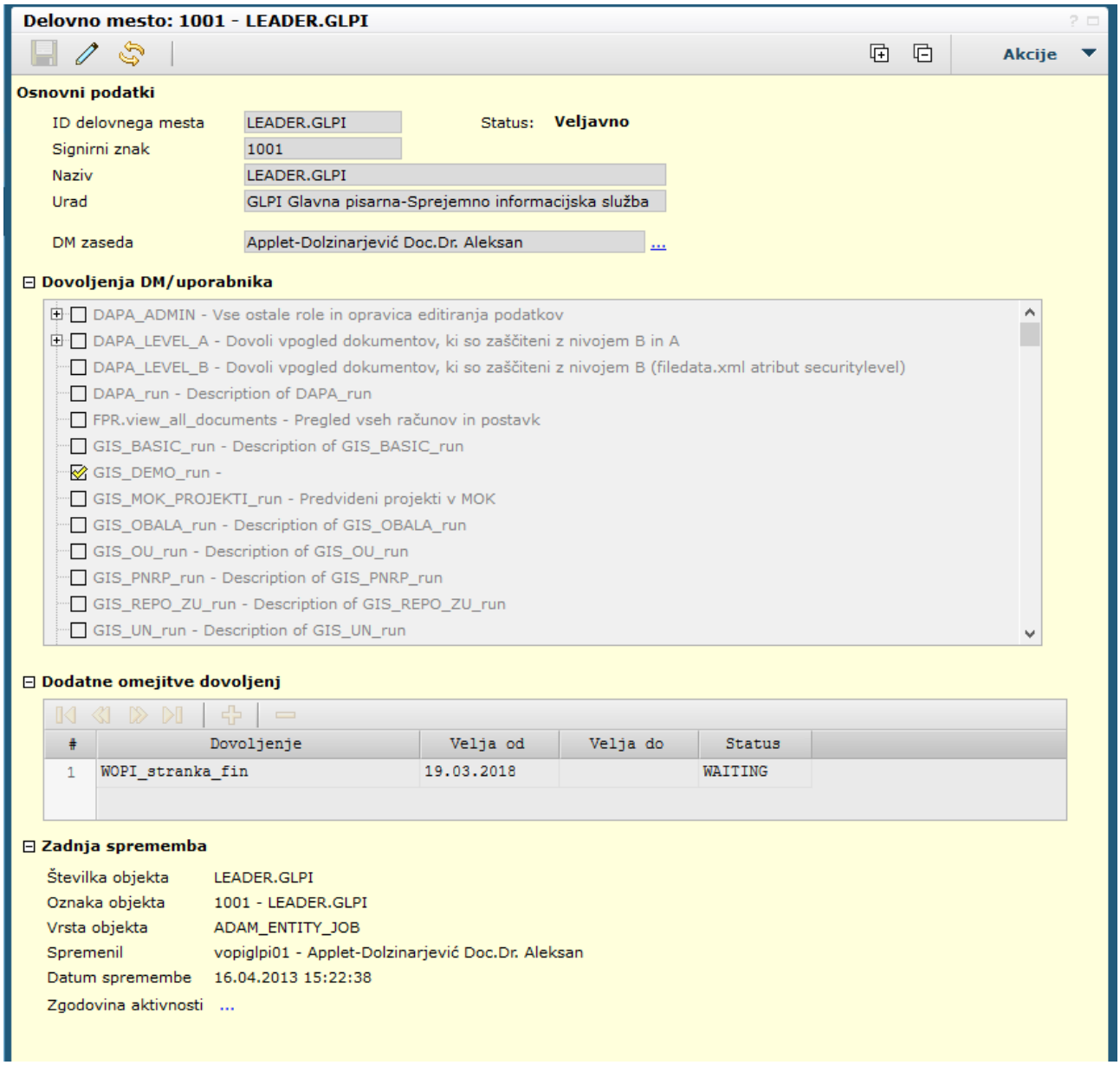
b) določanje pravic dostopov do posameznih delov/funkcionalnosti aplikacije temu uporabniku na tem delovnem mestu(delo s podatki):



c) določanje pravic izvajanja akcij nad podatki v bazi:



d) omejitev dostopa do posameznih možnosti oz. funkcij do določenega datuma ali po določenem datumu:



4. ADAM in revizijske sledi

ADAM prav tako beleži, uporabniški vmesnik pa prikazuje revizijsko sled dela s podatki v ADAM-u (Glej na predhodni sliki rubriko "Zadnja sprememba").

Revizijska sled se vodi na več nivojih:

- **DocRep knjižnica** ščiti dostope do posameznih objektov v aplikaciji glede na dodeljene pravice v ADAM-u ter beleži revizijsko sled dostopov do dokumentov in objektov. Vpogled v sled se vključi v vsako aplikacijo preko ADAM-a (različni uporabniški nivoji pravic vpogledov). Detajlnejši opis glej splošno navodilo "**DocRep - Orodja in delo z aplikacijami za delo z dokumenti tip "Skladišče dokumentov"**, poglavje "Zgodovina mojih aktivnosti"

- **Spletna aplikacija** ščiti dostop do aplikacije in do podatkov v aplikaciji glede na dodeljene pravice v ADAM-u ter beleži vse izvedene akcije v aplikacijah v revizijsko sled.
- **DBDS shramba dokumentov** ščiti dostop do datotek v bazi glede na dodeljene pravice v ADAM-u ter beleži revizijsko sled vseh dostopov in akcij nad datotekami. Vpogled v sled je omogočen pooblaščenim uporabnikom z uporabo orodja iQplus/DBDS. Detajlnejši opis glej navodilo "**iQplus/DBDS - Pregled nad dostopi do dokumentov v enotnem repozitoriju".** Ob namestitvi aplikacije in podatkovne baze administrator sistema vključi beleženje revizijske sledi, ki beleži vsa dejanja na sistemu DBDS. To izvede s konfiguracijsko tabelo. V DBDS sistemu so požilci (triggerji), ki prožijo pisanje revizijske sledi. Ponastavljanje nastavitev revizijske sledi ni možno zaradi varnostnih razlogov.

3 PORT Koper
ADAM navodilo v.3.0
operativa@3-port.si
16.03.2018