Nabava sustava za dodjeljivanje i upravljanje infrastrukturnim resursima ustanova i korisnika

Tehnička dokumentacija

Sadržaj

[1. Uvod 3](#_Toc45115705)

[1.1. Komponente sustava CARNET omega 3](#_Toc45115706)

[2. Pregled informacijskog sustava CARNET omega 6](#_Toc45115707)

[2.1. Opis središnjeg sustava za upravljanje CARNET omega 7](#_Toc45115708)

[2.1.1. Uloge korisnika 7](#_Toc45115709)

[2.1.2. Funkcionalni zahtjevi sustava 8](#_Toc45115710)

[2.1.3. Procesi središnjeg sustava za upravljanje CARNET omega 10](#_Toc45115711)

[2.2. Sustav za upravljanje elektroničkom poštom 11](#_Toc45115712)

[2.2.1. Osnovne funkcionalnosti 12](#_Toc45115713)

[2.2.2. Sastavne komponente sustava 13](#_Toc45115714)

[2.2.3. Ostali zahtjevi sustava za upravljanje elektroničkom poštom 14](#_Toc45115715)

[Performanse sustava trebaju biti takve da je moguće sljedeće: 14](#_Toc45115716)

[2.3. Sustav za upravljanje sadržajem mrežnih (*web*) stranica (CMS) 14](#_Toc45115717)

[2.3.1. Proces aktivacija CMS iz središnjeg sustava za upravljanje CARNET omega 14](#_Toc45115718)

[2.3.2. Funkcionalni zahtjevi CMS sustava 14](#_Toc45115719)

[2.3.3. Migracija sadržaja 16](#_Toc45115720)

[2.4. Sustav za upravljanje računalnom infrastrukturom dostupnom na zahtjev 16](#_Toc45115721)

[2.5. Sustav za dijeljenje i upravljanje dokumentima („fileshare sustav“) 17](#_Toc45115722)

[2.6. Sustav za upravljanje DNS zapisima 17](#_Toc45115723)

[2.7. Sustav za upravljanje uslugama u javnom oblaku za edukacijske ustanove 17](#_Toc45115724)

[2.8. Zajednički funkcionalni i tehnički zahtjevi sustava za upravljanje resursima 18](#_Toc45115725)

[2.8.1. Standardiziran front-end (engl. Unified Front - End, UFE) 19](#_Toc45115726)

[2.8.2. Performanse Rješenja 20](#_Toc45115727)

[2.8.3. Vizualni prikaz front-end-a 20](#_Toc45115728)

[2.8.4. Upravljanje zapisima (engl. Log Management) 20](#_Toc45115729)

[2.9. Usluge implementacije i održavanja sustava 21](#_Toc45115730)

[2.9.1. Radovi i rokovi implementacije sustava 21](#_Toc45115731)

[2.9.2. Radovi održavanja sustava 22](#_Toc45115732)

[2.9.3. Edukacija korisnika 22](#_Toc45115733)

[2.10. Obaveze Naručitelja 22](#_Toc45115734)

[2.10.1. Hardver i mrežni resursi 22](#_Toc45115735)

[2.10.2. Zajedničke funkcionalne komponente rješenja i postojećih sustava Naručitelja 23](#_Toc45115736)

[2.11. Očekivane aktivnosti od ponuditelja uključuju: 23](#_Toc45115737)

[2.12. Programski kod i programski jezici 23](#_Toc45115738)

[2.12.1. Alat za upravljanje izvornim kodom (engl. *Source Code Management, SCM*) 24](#_Toc45115739)

[2.12.2. Alat za kontinuiranu integraciju (engl. *Continuous Integration, CI*) 24](#_Toc45115740)

[2.13. Mikroservisna arhitektura 24](#_Toc45115741)

[2.13.1. Sustav za kontejnerizaciju 25](#_Toc45115742)

[2.13.2. Operativni sustav 26](#_Toc45115743)

[2.13.3. Infrastruktura 26](#_Toc45115744)

[2.14. Vlasništvo nad izvornim kodom i korisnička dokumentacija 26](#_Toc45115745)

[2.15. Komunikacija na projektu i nadzor provedbe ugovora 26](#_Toc45115746)

[2.16. Sigurnost informacijskog sustava za upravljanje resursima CARNET omega 27](#_Toc45115747)

[2.16.1. Sigurnost po dizajnu 27](#_Toc45115748)

[2.16.2. Sigurnosno testiranje sustava 27](#_Toc45115749)

[2.16.3. Uklanjanje uočenih sigurnosnih propusta 28](#_Toc45115750)

[2.16.4. Opseg sigurnosnog testiranja sustava 28](#_Toc45115751)

[3. Prilog A 30](#_Toc45115752)

[3.1. Postojeći sustavi 30](#_Toc45115753)

[3.2. Sustav za upravljanje elektroničkim identitetima korisnika 31](#_Toc45115754)

# Uvod

Program e-Škole dio je sveobuhvatnog programa modernizacije hrvatskog školskog sustava naziva “e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće”.

Opći cilj programa e-Škole pridonosi jačanju kapaciteta osnovnoškolskog i srednjoškolskog obrazovnog sustava, s ciljem osposobljavanja učenika za tržište rada, daljnje školovanje i cjeloživotno učenje.

Program e-Škole se provodi kroz sljedeće faze:

* I faza - Pilot projekt „e-Škole: Uspostava sustava razvoja digitalno zrelih škola" – trajanje od 1. ožujka 2015. godine do 31. kolovoza 2018. godine u koji je bilo uključeno 151 škola diljem Hrvatske
* II faza - predviđene aktivnosti razvijaju se na temelju iskustva i rezultata I faze (pilota), provodi se od 1. rujna 2018. godine do kraja 2022. godine i uključuje sve škole u Republici Hrvatskoj.

Nositelj projekta je Hrvatska akademska i istraživačka mreža - CARNET. Mjerodavno tijelo koje je nadležno CARNET-u je Ministarstvo znanosti i obrazovanja kojemu je nadležna Vlada RH. Projekt se financira sredstvima iz Europskog fonda za regionalni razvoj (EFRR) u sklopu Operativnog programa ''Konkurentnost i kohezija'' (OPKK) i iz Europskog socijalnog fonda (ESF) u sklopu Operativnog programa ''Učinkoviti ljudski potencijali'' (OPULJP) te je iz tog razloga je svaka faza programa dodatne podijeljena na Projekt A (sufinanciran sredstvima EFRR) i Projekt B (sufinanciran sredstvima ESF).

Planom projekta A u II fazi predviđena je implementacija sustava za dodjeljivanje i upravljanje infrastrukturnim resursima ustanova i korisnika (dalje CARNET omega sustav) opisa:

* Sustava za dodjeljivanje infrastrukturnih resursa i upravljanje udomljavanjem CARNET-ovih usluga u sklopu koje se svim školama, njihovim zaposlenicima, nastavnicima i učenicima otvara besplatan elektronički identitet i e-mail adresa, a školama je omogućena i izrada web stranica. Cilj je uspostaviti hosting uslugu nove generacije na najnovijim tehnologijama, optimiziranom potrošnjom resursa, unaprijeđenom i unificiranom administracijom od strane korisnika i CARNET-a.

## Komponente sustava CARNET omega

Slijedom napretka tehnologije s jedne strane, te promjena u zahtjevima od strane korisnika i aplikacija s druge, a temeljem revizije postojećeg sustava HUSO[[1]](#footnote-2) i povezanih usluga cilj je uspostaviti novu uslugu **CARNET omega** za dodjeljivanje i upravljanje infrastrukturnim resursima ustanova i korisnika.

CARNET omega objedinit će funkcionalnosti dosadašnjih komponenti i omogućiti jednostavniju administraciju i održavanje, otvoriti mogućnost efikasnijeg proširenja sustava s dodatnim uslugama za korisnike.

CARNET omega sustav se sastoji od više informacijskih podsustava koji zajedno čine integralnu cjelinu:

1. Središnja administratorska aplikacija za upravljanje CARNET omega podsustavima
	* središnje mjesto preko kojeg administratori pristupaju svojim uslugama i upravljaju resursima i svim podsustavima CARNET omega za svoju domenu
2. Upravljani sustav elektroničke pošte korisnika
3. Sustav za upravljanje sadržajem mrežnih (*web*) stranica (*Content Management System* - CMS)
4. Sustav za upravljanje DNS zapisima
	* za ustanove osnovnih i srednjih škola u Republici Hrvatskoj
5. Sustav za upravljanje alatima i uslugama u javnom oblaku za krajnje korisnike (kao npr. Microsoft 365 ili Google G Suite)
6. Upravljani sustav za dijeljenje dokumenata (*fileshare* sustav) i upravljanje dokumentima (DMS)
7. Sustav za upravljanje računalnom infrastrukturom dostupnom na zahtjev
	* komponenta sustava koja korisnicima omogućuje samostalnu izradu i administraciju virtualnih poslužitelja

CARNET omega namijenjen je:

* CARNET-ovim ustanovama članicama iz sustava osnovnoškolskog i srednjoškolskog obrazovnog sustava Republike Hrvatske
* Nastavnicima i učenicima osnovnoškolskog i srednjoškolskog obrazovnog sustava Republike Hrvatske

Uz CARNET omega, planom projekta A u II fazi predviđena je implementacija sljedećih sustava s kojima će sustav CARNET omega razmjenjivati podatke:

* Sustav za sigurno upravljanje matičnim podacima korisnika (GDPR 360)
	+ Sustav za sigurno upravljanje matičnim podacima korisnika u svrhu konzistencije i ostvarivanja tehničkih preduvjeta za ispunjavanja pravnih obaveza (GDPR regulativa). Uključuje pripremu osnovnih (matičnih) podataka svih sudionika CARNET usluga, potrebna proširenje imeničkih servisa, koji sadrži identitete korisnika i ustanova (CARNET Alpha sustav), implementaciju sustava za izradu jedinstvenog središnjeg skupa korisničkih privola, procese prikupljanja i povlačenja privola korisnika, automatizaciju pravila i provođenja GDPR zahtjeva za ispunjenje prava korisnika, te sinkronizaciju promjena privola pojedinog korisnika između više IT sustava.
* Aplikacija za jednostavnu autentifikaciju (CARNET FI)
	+ Aplikacija podršku sustavu za brzu i jednostavnu autentifikaciju krajnjih korisnika, prilagođenu njihovom uzrastu, namijenjena prvenstveno omogućavanju brze i jednostavne identifikacije i autentifikaciji učenika prilikom korištenja računalne opreme i IKT-a u nastavi.
* Nadogradnja Sustava za upravljanje API pozivima
	+ Sustav za upravljanje API pozivima osigurava jednostavnije upravljanje API pozivima s jednog mjesta, jednostavnije upravljanje pravima pristupa nad pojedinim servisima, povećanje sigurnosti uvođenjem novog komunikacijskog sloja među aplikacijama i mogućnost dizajniranja novih API poziva na samom sustavu uporabom postojećih pozadinskih sustava, integracijom s novim razvijenim servisima, kontroliranom razmjenom ili prikupljanjem podataka i skalabilno dograđivanje budućih sustava s novim tehnološkim rješenjima.
* Nadogradnja ekosustava za analitiku učenja
	+ Sustav za analitiku učenja (jezero podataka, skladište podataka i sustav za poslovne analize podataka i korisnička aplikacija Delta) uključuje dohvat podataka, propagaciju podataka i atributa prema skladištu podataka, transformaciju i pripremu za analitiku, nadogradnje sustava Delta s novim funkcionalnostima u skladu s potrebama krajnjih korisnika, izradu novih izvještaja prema potrebama dionika.

Uz razmjenu podataka između sustava koji će se razviti unutar projekta, CARNET omega razmjenjivati podatke sa sljedećim sustavima:

* e-Matice: <https://www.carnet.hr/projekt/e-matica/>
* Up2U: <https://learn.up2university.eu/>

Povezivanje CARNET omega podsustava, povezivanje podsustava i središnja administratorska aplikacija za upravljanje i povezivanja među ostalim sustavim iz II. faze projekta predviđeno je putem API sučelja koje će treba biti definirano i implementirano za svaku komponentu sustava.

# Pregled informacijskog sustava CARNET omega

CARNET Omega je okosnica CARNET-ovih korisničkih sustava i omogućuje upravljanje povezanim infrastrukturnim podsustavima pružanje usluga krajnjim korisnicima.



Slika 1- Shema informacijskog sustava CARNET Omega

## Opis središnjeg sustava za upravljanje CARNET omega

Središnja administratorska aplikacija za upravljanje CARNET Omega podsustavima upravlja svima sustavima i podsustavima s jednom mjesta i treba omogućiti upravljanje:

* elektroničkim identitetima korisnika koji uključuje
	+ upravljanje životnim ciklusom identiteta korisnika od kreiranja, promjena i brisanja iz sustava
	+ upravljanje LDAP atributima u sustavu CARNET alfa[[2]](#footnote-3)
	+ upravljanje lozinkama elektroničkih identiteta
* sustavom elektroničke pošte koji uključuje:
	+ webmaila
	+ postavke kao "mail aliase" i mailing liste
	+ upravljanje prosljeđivanjem do odredišnog sandučića e-pošte
* sustavom za upravljanje DNS zapisima za sve ustanove osnovnih i srednjih škola u Republici Hrvatskoj
	+ upravljanje primarnim i sekundarnim domenama
	+ upravljanje DNS zapisima za usluge na domeni
* servisima i korisničkim postavkama javnih usluga u oblaku uključujući
	+ upravljanje životnim ciklusom i aktivaciju korisničkog računa u javnom oblaku
	+ upravljanje korisničkim usluga u javnom oblaku
	+ Usklađivanje korisnički usluga koje su pružaju u javnom oblaku i u CARNET infrastrukturi
* sustavom za upravljanje *web* sadržajem - CMS
* sustavom za korisnike za dijeljenje dokumenata (fileshare sustav) i upravljanje dokumentima (DMS)
* Sustav za upravljanje računalnom infrastrukturom dostupnom na zahtjev

CARNET omega svim navedenim podsustavima treba upravljati putem sučelja za programiranje aplikacija (API, *engl. application programming interface*) odnosno putem standardnih protokola.

Osnove funkcije administratorske aplikacija sustava u upravljanju elektronički identitetima korisnika su:

* ažuriraju podaci o školi (adresa, broj telefona, ...)
* vrši unos i ažuriranje popisa učenika, nastavnog osoblja i drugog školskog osoblja
* pretražuju korisnici
* premještaju korisnici (npr. učenici iz osnovne škole u srednju)
* vrši izmjena/generiranje lozinki

Popis obveznih i neobveznih podataka škole i korisnika kao i detaljni opis i format zapisa svakog podatka može se pronaći na adresi: <http://shema.aaiedu.hr/shema/> .

### Uloge korisnika

Korisnici središnja administratorska aplikacija za upravljanje CARNET omega dijele se u četiri uloge:

* administratori CARNET omega usluge – AU
* administratori škole – AŠ
* administratori imenika - AI
* administratori resursa – AR

Administrator usluge (AU) je uloga CARNET-a, i odnosi se unos osnovnih podataka u sustav iz matičnih sustava nadležnog ministarstva, potrebnih da bi sustav za dodjeljivanje i upravljanje infrastrukturnim resursima ustanova i korisnika raspolagao s nužnim inicijalnim podacima na funkcioniranje. Administrator usluge treba moći upravljati svim sustavima i podsustavima kao i administratori imenika, administratori resursa i administratori škole za svaku školu posebno.

Svaka škola ima administratora škole (AŠ), a administrator škole može dodijeliti ovlasti administratora imenika (AI) i administratora resursa (AR) drugim korisnicima u sustavu. Administrator škole je osoba koja obavlja zadatke administratora imenika i administratora resursa, a korisnik u sustavu može imati više rola istovremeno.

Administratori imenika (AI) su zaduženi za ažurno održavanje popisa učenika, nastavnog osoblja i drugog školskog osoblja. Potrebno je ažurno održavanje obveznih podataka korisnika kao i podataka o školi (detaljnije informacije o obveznim podacima potražite na internetskoj adresi: <http://shema.aaiedu.hr/shema/> ) a sve u skladu s autentikacijskom i autorizacijskom infrastrukturom za obrazovni sustav RH.

Administratori imenika ažuriraju imenike, odnosno:

* dodaju nove korisnike, učenike i nastavnike,
* korisnicima kojima je istekao status u školi, unose podatak Datum isteka temeljne povezanosti.

Po nastupu promjena, Administratori imenika također ažuriraju i stanje imenika (npr. Dolazak/odlazak novog profesora ili učenika u/iz škole).

Administratori resursa (AR) zaduženi su za:

* kreiranje i mijenjanje grupnih aliasa
* upravljanje web stranicom škole
* upravljanje računalnom infrastrukturom dostupnom na zahtjev
* upravljanje informacijama o domenskom zapisu i sustavu elektroničke pošte za škole
* praćenje statistika.

### Funkcionalni zahtjevi sustava

#### Prijava u sustav

Administratori (AI, AR, AŠ, AU) se prijavljuju u sustav sa svojim korisničkim imenom i odgovarajućom lozinkom iz imeničkog sustava za skole.hr domenu (ID skole.hr). Svakom administratoru sučelje treba biti u skladu s njegovim ovlastima, odnosno sustav mu treba omogućiti upravljanjem entitetima i resursima za koje je zadužen.

Nakon uspješne prijave, administratoru škole treba biti omogućeno upravljanje sljedećim cjelinama:

* Škola – omogućuje promjenu podataka o školi i grupni unos korisnika
* Korisnici – omogućuje pregled korisnika (učenika i djelatnika) te dodavanje korisnika u školu i promjenu zajedničkih podataka
* Premještaj korisnika – omogućuje premještanje korisnika iz jedne škole u drugu, npr. nakon završene osnovne škole učeniku istekne status u osnovnoj školi, a administrator u srednjoj školi, pomoću imena i prezimena ili OIB-a, nalazi učenika i premješta ga u srednju školu
* Grupni aliasi – omogućuje dodavanje novog grupnog aliasa i promjenu postojećih grupnih aliasa
* Web – omogućuje promjenu vrste weba (statički web ili web upravljan CMS-om), upravljanje DNS zapisima za školu
* Statistike – omogućuje pregled statistika
* Odjava – omogućuje odjavu iz sustava

#### Izbornik o školi

Izbornik o školi omogućava:

* Pregled podataka o školi
* Promjenu podataka o školi
* Grupno kreiranje korisnika škole.

Obvezni podaci istaknuti su na obrascu masnim slovima. Sve matične podatke ustanove unosi Administrator usluge (AU) prilikom dodavanja škole u sustav.

 Prilikom promjene podataka o školi, svi obvezni podaci moraju biti navedeni (popis obveznih i neobveznih atributa hrEduOrg imeničke sheme nalaze se na adresi: <http://shema.aaiedu.hr/shema/> ).

Minimalni skup obveznih podataka za škole su:

* Identifikator ustanove – podatak koji se automatski generira prilikom dodavanja škole u sustav, jedinstven je u sustavu te nije moguće promijeniti njegovu vrijednost (Promjenu identifikatora može izvršiti samo AU)
* Naziv matične ustanove – ovaj se podatak odnosi na puni naziv ustanove, unosi ga AU
* Brojčani identifikator ustanove – identifikator prema kategorizaciji Ministarstva znanosti i obrazovanja (MZO)
* Poštanska adresa – službena adresa ustanove
* Mjesto – mjesto u kojem se nalazi ustanova;
* Elektronička adresa – službena elektronička adresa ustanove
* Tip ustanove – tip ustanove prema kategorizaciji Ministarstva znanosti i obrazovanja (MZO) (popis dozvoljenih vrijednosti možete pronaći na adresi: http://shema.aaiedu.hr/sifrarnici/org.php?prikazi=hrEduOrgType);
* URL adresa ustanove – URL adresa, mrežno sjedište ustanove.

Neobvezni podaci o školi su:

* Poštanski broj – poštanski broj iz službene adrese prema službenoj poštanskoj normi
* Ulica i kućni broj – ulica i kućni broj službene adrese
* Telefonski broj – telefonski broj ustanove
* Fax broj – broj telefaksa ustanove
* Broj mobilnog telefona – broj mobilnog telefona ustanove
* Pripadnost ustanovi – pripadnost nekoj ustanovi (npr. područne škole pripadaju nekoj matičnoj školi)
* URI adresa politike – vodi na stranicu s osnovnim načelima ustanove koja se odnose na zaštitu privatnosti korisnika.

Neobavezni set podataka je moguće proširiti s podacima o školama koji će biti dostupni prilikom izvođenja projekta implementacije sustava.

#### Upravljanje informacijama o domenskom zapisu i sustavu elektroničke pošte za škole

Za upravljanje informacijama o domenskom zapisu i sustavu elektroničke pošte za škole nadležan je podsustav za upravljanje DNS zapisima i treba biti moguće dodati sekundarnu domenu i zapis o poslužitelju elektroničke pošte (MX zapis) za sekundarnu domenu.

Sekundarna domena se koristi za škole koje otprije ima registriranu domenu u domenskom prostoru .hr, te je potrebno da domena vodi i na resurse novih servisa (web i drugo).

#### Statistike

Administrator resursa treba imati pristup statistikama koje prikazuju trenutačno stanje svakog korisnika u školi: statistike korištenje usluga u vremenu (najviše do godine dana), zauzetost resursa po uslugama i informacije o zadnjem uspješnom pristupu uslugama. Statistike trebaju biti dostupne putem API-a.

#### Odjava

Administratori se iz sustava se odjavljuju odabirom poveznice „Odjava“.

### Procesi središnjeg sustava za upravljanje CARNET omega

#### Izdavanje korisničkih podataka postojećim korisnicima

Korisnički podaci mogu se izdati postojećim korisnicima. Korisnikova lozinka može se, iz sigurnosnih razloga, izdati samo ako se generira nova. Ako se korisniku ne generira nova lozinka, dokument s korisničkim podacima ne sadrži lozinku.

#### Postupak za promjenu lozinke:

Administratori mogu mijenjati lozinke korisnicima na dva načina:

1. automatska promjena lozinke – sustav generira lozinku,
2. promjena lozinke – administrator može upisati lozinku koja treba zadovoljavati sigurnosna pravila.

Dodatno, sustav za upravljanje resursima ustanova CARNET omega treba omogućiti krajnjim korisnicima automatski opravak lozinke (odnosno izmjenu lozinke) na siguran način uzimajući u obzir zaštitu osobnih podataka i sigurnost sustava u cjelini.

#### Premještaj korisnika iz jedne škole u drugu školu

Premještaj učenika i drugih korisnika odnosi se na premještanje korisnika iz jedne škole u drugu. Važno je naglasiti da se mogu premještati samo oni korisnici kojima je istekao status u ustanovi iz koje ih se premješta (npr. nakon završene osnovne škole). Kod premještaja korisnika potrebno je unijeti jedan od podataka o korisniku kojeg želimo premjestiti: Ime i prezime, Identifikator korisnika u ustanovi, OIB.

Premještanje uvijek izvršava administrator škole u koju se korisnik premješta. Administrator škole iz koje učenik odlazi vidi samo korisnike svoje škole i ne može svoje korisnike dodavati u druge škole.

#### Promjena podataka o elektroničkom identitetu

Promjene podataka elektroničkog identiteta odnosi se na izmjene vrijednosti atributa u skladu s imeničkim shemama AAI@EduHr koji između ostalog uključuju ime korisnika, prezime korisnika, datum isteka temeljne povezanosti, i drugo.

Pri procesima premještaja korisnika i promjene elektroničkih identiteta treba definirati ponašanje elektroničkog identiteta i ovlasti i prava, a u vezi sa:

* Sinkronizacijom identiteta usluga u javnom oblaku
* Pravima korištenja usluga danih kroz sustav za upravljanje
	+ Primanje pošte
	+ Čitanje pošte
	+ Korištenje webamaila
	+ Upravljanje resurisma kao administrator
	+ Mogućnost korištenja sustava autentikacije i autorizacije

#### Promjena zajedničkih podataka korisnika

Sustav treba omogućiti promjene zajedničkih podataka za više korisnika odjednom (na primjer datum isteka temeljene povezanosti za učenike jednog razreda).

Administrator treba moći izvršiti pretragu korisnika i odabrati korisnike kojima će mijenjati zajedničke podatke, zaključati odabrane korisnike ili označiti ih za brisanje. Akcija promijene zajedničkih podataka omogućava promjenu zajedničkih podataka samo odabranim korisnicima.

Akcijom zaključavanja i brisanja administrator može svim odabranim korisnicima automatski promijeniti lozinku i onemogućiti korištenje korisničkog računa, odnosno označiti za brisanje samo odabrane korisnike.

Promjenom zajedničkih podataka korisnika, lozinke korisnika ostaju nepromijenjene i nisu vidljive u ispisu ili PDF dokumentu koji se generira.

#### Unos novih korisnika

Za učenike koji upišu školu i djelatnike koji se zaposle u školi a nemaju otvoren elektronički identitet potrebno je omogućiti unos (dodavanje) korisnika škole putem obrasca s poljima za unos obaveznih podataka korisnika. Obavezni podaci učenika i djelatnika, koji nisu testni računi ili sistemski, mogu se upisati isključivo dohvatom podataka iz sustava e-Matica i u skladu sa sustavom upravljanja matičnim podacima. Korisnici s Neobavezni podaci trebaju se moći upisati prilikom otvaranja elektroničkog identiteta ili naknadno kada je elektronički identitet već otvoren.

Kreiranjem korisnika automatski se stvaraju i dvije adrese elektroničke pošte. Prva adresa je oblika Ime.Prezime@identifikator-ustanove.skole.hr[[3]](#footnote-4), ili adresa Ime.PrezimeXX@ identifikator-ustanove.skole.hr, gdje je XX redni broj pojavljivanja identične adrese e-pošte. Druga adresa je alias oblika Ime.Prezime@skole.hr, odnosno Ime.PrezimeXX@skole.hr. Ova je adresa vezana za korisnika bez obzira kojoj ustanovi pripada i prati ga tijekom školovanja.

Na kraju postupka dodavanja novog korisnika je potrebno je moći ispisati podatke korisnika sa svim korisničkim podacima uključujući i lozinku.

Kod unosa novih korisnika sustav mora uskladiti procese sa sustavom za upravljanje matičnim podacima na način da su matični podaci korisnika jedinstveni na razini sustava za upravljanje resursima.

#### Brisanje elektronički identiteta

Brisanje elektroničkih identiteta treba se moći napraviti na dvije razine

* Označavanje korisnika za brisanje
* Trajno brisanje elektroničkog identiteta iz sustava

Pri procesima brisanja elektroničkih identiteta posebnu pozornost treba definirati ponašanje elektroničkog identiteta i ovlasti i prava, a u vezi sa:

* Sinkronizacijom identiteta usluga u javnom oblaku
* Pravima korištenja usluga danih kroz sustav za upravljanje
	+ Primanje pošte
	+ Čitanje pošte
	+ Korištenje webmaila
	+ Upravljanje resursima kao administrator
	+ Mogućnost korištenja sustava autentikacije i autorizacije
* Brisanjem poštanskog pretinca

## Sustav za upravljanje elektroničkom poštom

Sustav elektroničke pošte za osnovne i srednje škole potrebno je zamijeniti sustavom elektroničke pošte baziranog na softveru otvorenog koda koji podržava standardne protokole za čitanje i slanje elektroničke pošte (minimalno SMTP, IMAP, POP), aliase adresa elektroničke pošte (mail aliase) i e-mail liste, te sustav za čitanje i slanje elektroničke pošte putem web sučelja (webmail).

U pozadini sustav mora biti horizontalno skalabilan za svaku komponentu sustava elektroničke pošte. U prikazu korisnicima, sustav mora biti intuitivan i dostupan s mobilnih uređaja bez potrebe za instalacijom dodatnih aplikacija. Izvorni kod sustava elektroničke pošte mora biti javno dostupan i dozvoljavati modifikacije izvornog koda.

Glavni ciljevi novog sustava:

* Svakom korisniku CARNET-a potrebno je omogućiti korištenje poštanskog pretinca na samom sustavu elektroničke pošte (e-mail mailbox) s definiranom kvotom za elektroničku poštu (mailbox quota).
* Sustav mora biti skalabilan za potrebe planiranog rasta količini elektroničkih poruka (minimalno 20 e-poruka dnevno / korisniku)
* Dizajn skalabilan za prihvat novih korisnika, funkcionalnosti i integracija i bez dodatnog troškova licenciranja
* Sustav distribuiran na više ravnomjerno opterećenih poslužitelja
* Izrada sigurnosnih kopija podataka moguća unutar 24h bez prekida rada sustava

### Osnovne funkcionalnosti

Osnovne funkcionalnosti koje sustav za upravljanje elektroničkom poštom treba sadržavati jesu:

* rješenje bazirano na otvorenom kodu koje se izvršava na GNU/Linux platformi (npr. Debian, Ubuntu)
* otvoreni kod serverskog rješenja sustava je javno dostupan
* licenca otvorenog koda poslužitelja je GPL (v2)
* broj korisnika sustav se može povećati bez plaćanja licenci.
* sustav mora omogućavati izlaganje podataka i upravljanje putem RESTful (representational state transfer) API (application programming interface) s minimalno sljedećim mogućnostima:
	+ dodavanje i upravljanje mail domenom (SMTP, IMAP, POP)
	+ dodavanje i upravljanje korisnicima na mail domeni
	+ dodavanje i upravljanje mailing listama na mail domeni
	+ upravljanje korisničkim postavkama kao povećanje quote i vraćanje obrisanih mailova
	+ upravljanje mail filterima
* rješenje dopušta pisanje ili korištenje dodataka (eng. *plug-in*) za proširivanje funkcionalnosti sustava
* rješenje dopušta korištenje putem klijenta e-pošte
* rješenje je lokalizirano i sučelje je na hrvatskom jeziku
* rješenje omogućava prilagodbu prema knjizi grafičkih standarda Naručitelja
* rješenje dopušta pretraživanje mailova po više parametara pretraživanja
* rješenje dopušta podešavanje i korištenje distribucijskih lista
* rješenje dopušta integraciju s ID sustavom skole.hr putem LDAP-a protokola i korištenje globalnih adresnih lista (GAL)
* rješenje omogućava korisnicima korištenje i upravljanje kalendarima, bilješkama i kontaktima
* rješenje podržava CardDav, CalDav i iCal klijente
* rješenje podržava Web administracijsku konzolu
* rješenje podržava komandno linijsko sučelje
* rješenje dopušta podešavanje maksimalnih kvota po tipovima korisničkih profila
* rješenje omogućava korisnicima korištenje i upravljanje postavka i filterima za automatsko odgovaranje na e-poštu
* responzivnost sučelja i pristup putem mobilne aplikacije za Android i IOS platforme
* dodavanje i upravljanje korisnicima sustava elektroničke pošte
* dodavanje i upravljanje domena na sustav elektroničke pošte
* upravljanje podržanim protokolima za čitanje i slanje elektroničke pošte (SMTP, IMAP, POP i slično)
* dodavanje i upravljanje mailing listama
* dodavanje i upravljanje mail aliasima
* upravljanje kvotama poštanskih sandučića
* upravljanje filterima elektroničke pošte
* upravljanje prosljeđivanjem elektroničke pošte
* kreiranje grupa i distribucijske lista u adresaru, na koje može poslati zajednička poruka
* prostor za pohranu korisničkih dokumenata
* integracija prijave sumnjivih e-mailova CERT-u
* postavljanje i trenutačna primjena kvota na razini pojedinog pretinca
* mobilni pristup na POP/IMAP/SMTP poslužitelj i njegove sigurne inačice te STARTTLS
* postavljanje kategorija korisnika u logičke grupe i zatim primjena različitih funkcionalnosti i limita nad tim grupama npr. protokol (IMAP/POP/…), kalendar, veličina kvote i sl.

### Sastavne komponente sustava

Od Ponuditelja se zahtjeva tehničko rješenje novog sustava uključujući dizajn, arhitekturu i dokaz rada koncepta sustava. Tehničko rješenje će se minimalno sastojati od sljedećih funkcionalnih kategorija poslužitelja:

* Kategorija Ulazni AV/AS poslužitelj
* horizontalna skalabilnost ulaznih AV/AS poslužitelja pomoću *LoadBalancera*
* usmjeravanje skeniranih mailova na višestruke MTA poslužitelje (bez ili pomoću *LoadBalancera*)
* provjera postojanja i lokacije mailboxa prije obrade mailova
* dinamička ili skriptabilna promjena konfiguracije za promjenu broja backend poslužitelja
* prilagodba filtriranja specifično za dolazeće mailove
* Kategorija Izlazni AV/AS poslužitelj
* horizontalna skalabilnost izlaznih AV/AS poslužitelja (bez ili pomoću *LoadBalancera*)
* prilagodba filtriranja specifično za odlazne mailove
* vidljivost pošiljatelja koji narušava reputaciju ustanove
* Kategorija poslužitelja za razmjenu e-pošte
* horizontalna skalabilnost poslužitelja za razmjenu e-pošte (MTA – Mail Transfer Agent)
* dinamicka ili skriptabilna promjena konfiguracije za promjenu broja izlaznih AV/AS poslužitelja
* dinamička ili skriptabilna promjena konfiguracije za promjenu broja Mailbox poslužitelja
* dinamička provjera lokacije korisnika na poslužiteljima sandučića e-pošte
* podrška konfiguracija redirekcije korisnika na uslugu e-pošte u javnom oblaku (minimalno Google G Suite i Microsoft Office365)
* Kategorija poslužitelj sandučića e-pošte (Mailbox poslužitelj)
* horizontalna skalabilnost poslužitelja sandučića e-pošte
* korištenje Ceph pohrane podataka za potrebe rada poslužitelja e-pošte ili za potrebe poslužitelja mail aplikacije
* mogućnost upravljanja podacima s obzirom na broj datoteka i s obzirom na korištenje Ceph storage (npr listanje, mogućnost backupa)
* mogućnost raspodjele novih korisnika po poslužiteljima sandučića e-pošte
* mogućnost migracije korisnika između poslužitelja sandučića e-pošte
* neovisan rad pojedinih poslužitelja sandučića e-pošte
* pristup vanjskom pružatelju identiteta s *read-only* pravima
* broj korisnika po poslužitelja sandučića e-pošte 50 000 - 100 000
* Kategorija LDAP poslužitelj
* horizontalna skalabilnost i visoka dostupnost LDAP poslužitelja mail sustava
* rasterećenje read operacija LDAP poslužitelja višestrukim slave replikama ili višestrukim master replikama
* Kategorija *caching* poslužitelj
* horizontalna skalabilnost *cache* sloja za autentifikaciju
* rasterećenje eksternog i internog izvora identiteta korisnika
* Kategorija webmail/webadmin poslužitelj
* horizontalna skalabilnost webmail/webadmin poslužitelja
* dinamička ili skriptabilna promjena konfiguracije za promjenu broja poslužitelja sandučića e-pošte
* dinamička provjera lokacije korisnika na poslužitelju sandučića e-pošte

### Ostali zahtjevi sustava za upravljanje elektroničkom poštom

### Performanse sustava trebaju biti takve da je moguće sljedeće:

* obrada minimalno 10 000 000 mailova u danu (zbrojeno ulaz i izlaz)
* korištenje ukupnog prostora za pohranu pretinaca elektroničke pošte od minimalno 1PB
* obrada minimalno 6000 paralelnih IMAP konekcija
* obrada minimalno 3000 paralelnih Webmail konekcija

## Sustav za upravljanje sadržajem mrežnih (*web*) stranica (CMS)

CMS omogućuje krajnjim korisnicima, kojima je dato pravo, da upravljaju sadržajem na web stranici, odnosno mijenjaju i dodaju fotografije, tekstualni ili video sadržaj te redovne objavljuju na blogu novosti i zanimljivosti iz svog okruženja.

S obzirom na veliki broj korisnika i značajnu količinu sadržaja koja je nastala u više od 10 godina korištenja sustava[[4]](#footnote-5), potrebno je voditi računa o zadržavanju postojećih funkcionalnosti i sadržaja u što je mogućoj većoj mjeri.

### Proces aktivacija CMS iz središnjeg sustava za upravljanje CARNET omega

Prijavom administratora resursa škole (AR), ukoliko se odabere CMS kao opcija, u sustavu se treba kreirati web stranica škole prema unaprijed definiranom predlošku. Izrada sadržaja i upravljanje sadržajem nakon toga imaju korisnici prema definiranim ovlastima u CMS-u. Automatizirani popisi učenika, djelatnika, razrednih odjela i strukture organizacije jedne škole trebaju biti usklađeni sa strukturom u sustavu e-Matica.

### Funkcionalni zahtjevi CMS sustava

Novo CMS rješenje mora omogućiti jednostavno upravljanje, održavanje i ažuriranje web stranica od strane administratora, odnosno kreiranje sadržaja od strane ovlaštenih korisnika.

U tom smislu Rješenje mora zadovoljavati minimalno sljedeće uvjete:

* Internetske stranice (webovi) škola putem sustava za upravljanje sadržajem treba moći postaviti i ažurirati na jednostavan, standardiziran i unaprijed definiran način pomoću web preglednika.
* rješenje bazirano na tehnologiji otvorenog koda koje omogućava Naručitelju izmjene izvornog koda i proširenja sustava bez kupovine licenci
* podršku za korištenje http/https protokola
* sustav mora biti organiziran hijerarhijski
	+ stranice svih škola moraju funkcionirati unutar istog sustava ali kao zasebne cjeline
	+ aplikativni dio dijeljen među cjelinama, ali neovisne baze podataka
	+ Uloge su složene po razinama, od glavnog administratora (CARNET), prema administratorima stranica škola
* svaka niža razina ima svog administratora koji definira prava korisnika za strukture niže razine
* sustav mora biti skalabilan - broj webova škola kao i broj webova razreda, učenika, itd. ne smije biti ograničen, kao niti broj korisnika i grupa korisnika, niti povezan s dodatnim troškovima licenciranja
* svaka škola mora moći samostalno birati između ponuđenih dizajnerskih rješenja i rješenja organizacije podataka ili samostalno definirati svoje vlastito rješenje unutar sustava
* funkcionalnosti će biti opcionalno predefinirane na svakom predlošku weba te se njihova daljnja uporaba prepušta pojedinoj školi što podsustav za upravljanje web sadržajem treba omogućiti.
* mogućnost grupiranja više web stranica u jedan sustav, ali i razdvajanje u zasebne cjeline, što mora omogućiti istovremeno instaliranje i ažuriranje svih web stranice u jednom sustavu,
* mogućnost definiranja administratora pojedinih web stranica koji će imati prava dodavati nove korisnike, ali samo za web stranice na kojima su administratori te aktivirati dodatke za svoje web stranice (ali ne i instalirati nove dodatke),
* mogućnost definiranja uloga i pripadajućih prava korisnika pojedine web stranice,
* mogućnost dodavanja i uređivanja sadržaja i navigacije isključivo putem web formulara ili *drag and drop* metode,
* mogućnost poboljšanja i izmjene funkcionalnosti, instaliranjem dodataka bez potrebe za dodatnim programiranjem, minimalno:
	+ Popis korisnih poveznica
	+ Često postavljana pitanja
	+ Repozitorij datoteka
	+ RSS reader
	+ Vijesti
	+ Banner
	+ Pretraživanje
	+ Kalendar
	+ Provođenje anketa
	+ Automatska karta web stranica
	+ Osobne stranice za učenika i nastavnika
	+ Blog
	+ Raspored sati
	+ Foto-album
	+ Oglasna ploča
* mogućnost odabira između više tema web stranice,
* administratorsko sučelje na hrvatskom jeziku,
* Responzivnost sučelja mobilnih web-stranica
* mogućnost usklađivanja sa Zakonom o pristupačnosti u kontekstu osiguravanja pristupačnosti Rješenja za pokretne uređaje korisnicima, osobito osobama s invaliditetom, uključujući zadovoljavanje minimalno sljedećih zahtjeva:
	+ mogućnost opažanja, što znači da sadržaj i sastavni dijelovi korisničkog sučelja moraju biti predstavljeni korisnicima na način da im omogućavaju opažanje,
	+ operabilnost, što znači da se sastavnim dijelovima korisničkog sučelja i navigacije mora moći upravljati
	+ razumljivost, što znači da informacije i način rada korisničkog sučelja moraju biti razumljivi,
* prilikom učitavanja datoteke Rješenje mora uz provjeru prema ekstenziji, provjeravati i zaglavlje datoteke (kako bi se izbjeglo da netko slučajno / namjerno učita maliciozni kod),
* mogućnost ograničavanja i kasnije izmjene, prilikom učitavanja na web stranice, maksimalnih veličina i rezolucija fotografija prema kategorijama (npr. mogućnost ograničavanja veličine i rezolucije za fotografije u galeriji na 800 x 600px i 150kB, popratnih fotografija teksta (engl. *Thumbnail*) na 150 x 150px i 8 kB, naslovnih fotografija objava na 1200 x 630px i 200kB, istaknutih fotografija (engl. *Featured Image*) na 800 x 600px i 150kB i sl.),
* prilikom učitavanja fotografija na web stranice, rješenje treba automatski obrisati sve EXIF informacije bez iznimke
* prilikom učitavanja fotografija na web stranice, rješenje treba podržati postavljanje ograničenja u veličini dodane fotografije ili automatski smanjiti veličinu na definiranu maksimalnu vrijednosti
* mogućnost obrezivanja (engl. *Crop*) fotografija prilikom učitavanja na web stranice,
* integrirani RSS čitač,
* mogućnost konvertiranja postojećih web stranica iz dinamičkog oblika u statički oblik – na što jednostavniji način (npr. intervencijom administratora pojedine web stranice),
* mogućnost pristupanja starijim verzijama sadržaja web stranica i objava bez potrebe za dodatnim programiranjem,
* mogućnost pretraživanja sadržaja web stranice po ključnoj riječi,
* mogućnost definiranja hijerarhije web stranice bez potrebe za dodatnim programiranjem i sl.
* mogućnost postavljanje i upravljanja obavijestima o prikupljanju korisničkih podataka i korištenju kolačića

### Migracija sadržaja

S obzirom na veliki broj korisnika i značajnu količinu sadržaja koja je nastala dosadašnjim korištenjem sustava, potrebno je voditi računa o zadržavanju postojećih funkcionalnosti i sadržaja u što je mogućoj većoj mjeri, a minimalno sadržaja nalazi se u modulima vijesti, dokumenti i fotografije.

Potrebno je predvidjeti i omogućiti paralelan rad obaju sustava u određenom periodu migracije.

Pokretanje migracije je na zahtjev – ukoliko škola odabere opciju korištenja novog CMS-a, kreira se novi web i nastavlja procedura ovisno o odabranoj opciji migracije sadržaja.

## Sustav za upravljanje računalnom infrastrukturom dostupnom na zahtjev

Sustav za upravljanje računalnom infrastrukturom dostupnom na zahtjev je podsustav u upravljanju informacijskim resursima ustanova u obrazovnom sustavu Republike Hrvatske, koji treba korisnicima omogućiti samostalnu izradu i administraciju virtualnih poslužitelja (VP), a uz sigurnosne komponente sustava potrebno je da sustav ima nadzora statusa pojedinog virtualnog računalnog poslužitelja i mogućnost da korisnici mogu samostalno upravljaju brojem, veličinom, odnosno kapacitetima virtualnih poslužitelja do definirane razine koju nadzire i njome upravlja sam sustav.

Zahtjevi za sustavom za upravljanje VP su:

* pokretanje i upravljanje instancama poslužitelja što uključuje upravljanje kapacitetima diska, CPU-a i radne memorije, te mogućnost "live" migracija
* upravljanje mrežnim postavkama u privatnom oblaku, vatrozidom (firewallom) i javnim IP adresama
* svaki VP korisnik treba dobiti svoj samostalni VLAN i upravljati firewallom do svog VLAN-a.
* korištenje operativnih sustava otvorenog koda ili krajnji korisnik treba osigurati vlastitu licencu na licencirano operativne sustave
* upravljanje sigurnosnim kopijama (backup) i "snapshotima" poslužitelja
* upravljanje „load balancerom“ u slučaju korištenja više poslužitelja
* nadzor i obavještavanje o statusu i performansama podignuti instanci, odnosno virtualnih poslužitelja
* VP ograničenja ukupnih angažiranih resursa: povećavanje postojećih i dodavanje novih poslužitelja moguće je do određene razine, do koje korisnik može sam upravljati veličinom i brojem poslužitelja. Razinu ukupnog angažmana računalnih resursa odradit će Naručitelj.

Svim navedenim zahtjevima potrebno je upravljati putem API poziva.

## Sustav za dijeljenje i upravljanje dokumentima („fileshare sustav“)

Podsustav za dijeljenje datoteka i upravljanje datotekama (DMS, engl. Document Management System) ima dvije ključne funkcionalnosti: mogućnost dijeljenja dokumenta između korisnika te upravljanje dokumentima u smislu praćenje životnog vijeka dokumenta od stvaranja dokumenta, promjena verzija dokumenata do arhiviranja dokumenta u jedinstvenom repozitoriju dokumenata.

U dijelu vezanom za dijeljenje dokumenata, sustav treba omogući dijeljenje dokumenta svim korisnicima sustava i prema potrebi korisnicima izvan CARNET, a pri tome zadržati sigurnost, privatnost, jednostavnosti korištenja i brzini slanja dokumenata. Dokumente treba moći dijeliti s pojedinačnim korisnikom ili definiranom grupom korisnika (npr. korisnici jedne ustanove ili korisnici iz više ustanova). Dio sustava koji se tiče upravljanja dokumentima treba imati svu kontrolu nad životnim ciklusom dokumenta i odnosi se na način na koji se dokumenti pohranjuju, sastavljaju iz više različitih dokumenata, prate kroz poslovni proces i upravljaju putem kontrolnih točaka u poslovnom procesu.

Važno je da sustav sadrži centralni repozitorij dokumenta (jedna instanca, odnosno jedna pojavnost dokumenta) koji omogućava dostupnost svih dokumenata kroz funkcionalnosti arhiviranja i pretraživanja.

Korisnici ovog podsustava su učenici, učitelji, djelatnici i ustanove članice.

Svim navedenim zahtjevima potrebno je upravljati putem API poziva.

## Sustav za upravljanje DNS zapisima

Sustav za upravljanje DNS zapisima kao informacijski podsustav sustava namijenjen je upravljanju DNS zapisa ustanova osnovnih i srednjih škola u Republici Hrvatskoj putem API poziva.

U okviru Sustava za upravljanje DNS zapisima minimalno moraju biti izgrađene sljedeće funkcionalnosti:

* dodavanje nove zone, brisanje zone,
* prikaz, dodavanje, brisanje zapisa,
* uvoz i izvoz zapisa iz datoteke,
* transfer DNS zone putem AXFR mehanizma
* bilježenje i prikaz povijesti izmjena zone,
* DNSSEC potpisivanje zone u svrhu potvrde izvornosti, integriteta i autentičnosti DNS podataka
* dodavanje sekundarnog poslužitelja za DNS zone
* definiranje gornje vrijednosti (kvote) za DNS zone,
* preusmjeravanje domene na drugu domenu.

Sustav za upravljanje DNS zapisima treba omogućiti dodavanje sekundarne domene i zapis o poslužitelju elektroničke pošte (MX zapis) za sekundarnu domenu kojim definira ime servera zaduženog za primanje e-pošte za sekundarnu domenu. Također, navedeni podsustav za upravljanje DNS zapisima treba biti izgrađen na način da se njime upravlja putem sučelja za programiranje aplikacija (API, application programming interface). Za buduće nadogradnje sustav treba biti proširiv na način da se može upravljati domenskim prostorom nacionalne vršne domene ".hr".

Svim navedenim zahtjevima potrebno je upravljati putem API poziva.

## Sustav za upravljanje uslugama u javnom oblaku za edukacijske ustanove

U okviru sustava potrebno je izgraditi podsustav za upravljanje alatima i uslugama u javnom oblaku za edukacijske ustanove kao što su Microsoft o365 ili Google G Suite. Sustav za upravljanje uslugama u oblaku treba omogućiti aktivaciju korisničkih računa u javnom oblaku i korištenje usluga koje su dane korisnicima na besplatno korištenje poput on-line pohrane podataka, korisničkog email sandučić velikog kapaciteta, uredske alate i alate za učenje na daljinu, te druge alate koje nude pružatelji usluga u javnom oblaku.

Upravljanje uslugama u javnom oblaku uz aktivaciju usluge podrazumijeva i upravljanje suglasnostima vezanim uz aktivaciju računa u javnom oblaku i korištenje usluga, te osnovno podešavanje usluge u javnom oblaku, ako je ono dostupno putem sučelja za programiranje aplikacija - poput definiranja e-mail sustava na kojem je otvoren poštanski pretinac (mailbox) korisnika.

Trenutno su omogućene usluge "Google G Suite for Education" i "Microsoft Office365 usluga", te se za navedene usluge treba omogućiti:

* aktivacija usluge,
* deaktivaciju usluge,
* i osnovno upravljanje uslugom koje uključuje i upravljanje privolama vezanim uz aktivaciju računa i korištenje usluga
* podršku konfiguracija redirekcije korisnika na uslugu e-pošte u javnom oblaku.

## Zajednički funkcionalni i tehnički zahtjevi sustava za upravljanje resursima

Korisnici sustava trebaju biti jedinstveni na razini sustava bez mogućnosti recikliranja elektroničkih identiteta ili adresa krajnjih korisnika, a adrese elektroničke pošte u ovom sustavu su adrese elektroničke pošte navedene u sustavu za elektroničkim identitete korisnika (CARNET alfa).

Važan dio funkcionalnosti koji cjelokupno rješenje treba imati jesu:

* mogućnost korištenja servisnih korisničkih računa
* mogućnost korištenja testnih korisničkih računa
* mogućnost korištenja jednog elektroničkog identiteta za djelatnike koji rade na više ustanova

S obzirom na planove razvoja IT sustava CARNET-a, sustavi moraju raditi sa Ceph SDS-a diskovnim sustavom kojeg konfigurira Naručitelj, te treba biti vidljiv razvojni put za prebacivanje komponenata sustava elektroničke pošte u kontejnere pod upravljanjem Kubernetes orkestratora kontejnera ili drugih izvedenica orkestratora baziranih na Kubernetesu.

U sklopu projekta potrebno je osigurati da se kompletan sustav može nadzirati s jedinstvene lokacije, koji će automatski dizati reaktivne alarme u slučaju problema ili proaktivno prije nego problem nastane. Također, potrebno je osigurati da je moguće pregledati operativne zapise (log) s cijelog sustava na jednom mjestu kako bi otklanjanje grešaka bilo brzo i efikasno. Skaliranje sustava prema gore ili prema dolje mora biti moguće automatizacijom, bilo ugrađenim funkcionalnostima softverom elektroničke pošte i/ili softverom za upravljanje konfiguracijama, uključujući na vezivanje na infrastrukturu za uspostavu novih virtualnih poslužitelja.

Sve komponente sustava moraju biti visoko dostupne.

Nadogradnja softverskih komponenti sustava mora biti moguća bez upliva na korisnike.

Zajednički zahtjevi za sve informacijske sustave i podsustave sustava za upravljanje resursima jesu:

* Koriste se rješenja i komponente bazirana na tehnologijama otvorenog koda
* Za komponente za koje ne postoji adekvatno rješenje bazirano na otvorenom kodu, potrebno je razviti prilagođeno rješenje, a kod kojeg postaje vlasništvo Naručitelja po završetku projekta
* Za komunikaciju podsustava međusobno, glavnog sustava CARNET omega sa svima podsustavima i međuslojevima koristiti REST API i standardne protokole
* Korištenje usluga treba biti mjerljivo što uključuje i definiranje KPI-a
* Podaci o korištenju sustava, dijelovi REST servisa te forme i widgeti trebaju biti dostupni portalu za korisnike i CARNET delta sustavu (jezeru podataka)
* Sustav mora bilježiti sistemske i korisničke aktivnosti na svim komponentama sustava i upravljati poslužiteljskim zapisima (Log Management)
* Sustav i sve komponente sustava trebaju biti nadogradive i skalabilne
* Sustav treba koristiti tehnologije koje podržavaju mikro-servisnu arhitekturu i arhitekturu kontejnera
* Posebna pozornost treba biti usmjerena na sigurnost sustava, svih komponenti i podsustavima
* Sustav mora biti u skladu s Općom uredbom o zaštiti osobnih podataka (Uredba (EU) 2016/679) i ostalim propisima kojima se uređuje zaštita osobnih podataka te primjenjivati metode i principe dizajna sustava i zaštite osobnih podataka koje Uredba i ostali propisi uređuju
* Uvažiti preporuke i smjernice za pristupačnost sadržaja (<https://www.carnet.hr/pristupacnost/>)

### Standardiziran front-end (engl. Unified Front - End, UFE)

UFE omogućuje korisnicima pristup Rješenju preko različitih uređaja koji podrazumijevaju različite veličine i rezolucije zaslona. Rješenje se mora ispravno prikazivati u različitim preglednicima (engl. cross-browser), na različitim operativnim sustavima (engl. cross-platform) i različitim uređajima (engl. cross-device). UFE definira programske jezike razvoja Rješenja. U sklopu UFE-a dodatno je definiran vizualni prikaz korisničkih i administratorskih sučelja Rješenja koji mora omogućiti korisnicima jednostavan pristup relevantnim informacijama u obliku koji je standardiziran i ujednačen za sve aplikacije u sklopu Rješenja. U nastavku su potkategorije UFE-a, svaka određenih funkcionalnosti / pretpostavke koje Rješenje minimalno mora zadovoljavati.

#### Kompatibilnost s operativnim sustavima

Mogućnost isporučivanja Rješenja na sljedećim operativnim sustavima (minimalan popis):

* Android,
* Chromium,
* iOS,
* OS X,
* Linux,
* Windows i sl.

#### Kompatibilnost s uređajima

Mogućnost isporučivanja Rješenja na sljedećim uređajima (minimalan popis):

* stolno računalo i laptop
* mobilni uređaj i tablet)

#### Kompatibilnost s web preglednicima nove generacije

Mogućnost isporučivanja Rješenja na sljedećim web preglednicima (minimalan popis):

* Chrome,
* Safari,
* Internet Explorer,
* Firefox,
* Edge i sl.

#### Jezik

Korisnička i administratorska sučelja ponuđenog Rješenja moraju biti dostupna na hrvatskom jeziku.

### Performanse Rješenja

Imajući na umu korisničko iskustvo i sve manju toleranciju korisnika na sporo učitavanje web stranica i web aplikacija, potrebno je osigurati dovoljno brzo učitavanje Rješenja, odnosno potrebno je zadovoljiti sljedeće uvjete:

* prilikom učitavanja, prva smislena boja se mora učitati ispod 1 sekunde,
* vrijeme za interakciju (engl. Time to Interactive) mora biti ispod 5 sekundi u mreži s 400ms RTT i 400kbps brzinom prijenosa i manje od 2 sekunde za ponavljanje posjeta te
* veličina kritične datoteke (engl. Critical File) mora biti ispod 170Kb Gzipped.

### Vizualni prikaz front-end-a

Rješenje mora imati mogućnost vizualne prilagodbe korisničkog i administratorskog sučelja organizaciji Naručitelja (dobavljaču će biti dostavljena knjiga grafičkih standarda Naručitelja). U tom smislu minimalno sljedeći elementi moraju biti u skladu sa standardima Naručitelja:

* stil stupaca (engl. Grid system) – širina, broj stupaca,
* poravnanje teksta,
* boje,
* font (veličina fonta i prored),
* stil linkova i navigacije (engl. default, hover, focus, active and visited state),
* veličine i oblici slika i ikona,
* forme i gumbi te
* skalabilni dizajn (engl. Responsive) web aplikacije – Rješenje pri veličini zaslona od 1008px i više mora biti u desktop prikazu, između 641 i 1007px u tablet prikazu, a pri veličini zaslona od 640px i manje u mobilnom prikazu.

### Upravljanje zapisima (engl. Log Management)

Upravljanje zapisima služi za nadzor i bilježenje sistemskih, administratorskih i korisničkih aktivnosti na svim komponentama sustava. Zapisi omogućavaju otkrivanje sigurnosnih incidenata i operativnih poteškoća sustava, odnosno postavljaju temelje za centralno upravljanje sigurnosnim događajima (engl. Security Information and Event Management, SIEM) što pretpostavlja prikupljanje, normaliziranje i automatiziranje analize sigurnosnih događaja i zapisa, generiranje konsolidiranih izvješća u realnom vremenu, omogućavanje grafičkih prikaza i pružanje upozorenja o sigurnosti cijelog sustava. Pri tome SIEM rješenje uzima u obzir korelaciju između navedenih sistemskih i korisničkih zapisa.

Kategorije zapisi koji se kreiraju na aplikacijama su:

* sistemski zapisi koji prikazuju određene događaje, statuse, mrežne konekcije i sl.,
* administratorski zapisi koji prikazuju izravne aktivnosti: na promjeni konfiguracije, manipuliranja podacima, konfiguriranju sigurnosnih postavki (autentikacija, autorizacija, upravljanje korisničkim računima, itd.) i sl.,
* korisnički zapisi koji prikazuju transakcije povezane s promjenom podataka npr. pristup određenog korisnika podacima na disku, bazi podataka i sl.

U nastavku su definirane minimalne strukture zapisa koje Rješenje mora bilježiti i lista događaja koji predstavljaju sigurnosne događaje i moraju biti zapisani na Rješenju.

#### Struktura zapisa koje Rješenje mora bilježiti

Odabrano Rješenje mora omogućiti slanje zapisa na centralni SIEM u JSON formatu. Rješenje mora osigurati da zapisi koji se šalju na SIEM imaju dovoljno informacija koje su nužne da se jednoznačno može odrediti minimalno sljedeće:

* tko je proveo određenu korisničku aktivnost:
	+ korisnički ID,
* od kud je aktivnost provedena:
	+ ime računala i/ili IP adresa,
	+ ime aplikacije,
* gdje je aktivnost provedena:
	+ imena datoteka,
	+ podatak kojem se pristupalo u bazi,
* kad je aktivnost provedena:
	+ datum i vrijeme (uključujući podatke o vremenskoj zoni, odmaku od UTC, GMT),
* koja je aktivnost provedena:
	+ tip aktivnosti (autorizacija, verifikacija, kreiranje, čitanje, pisanje, izmjena, brisanje, prihvat konekcije, itd.),
* koji je status (uspješno / neuspješno), ishod ili rezultat provedene aktivnosti:
	+ vrijednost prije i poslije, ukoliko se radi o izmjeni podataka, ako je to moguće,
	+ da li je aktivnost bila prihvaćena ili odbijena te
	+ objašnjenje ili kodirani zapis razloga zbog kojeg je provođenje aktivnosti odbijeno.

#### Lista događaja koje Rješenje mora bilježiti

Događaji koji predstavljaju sigurnosne događaje moraju se evidentirati i programski dohvatiti sa središnjeg sustava Naručitelja za evidenciju događaja. Minimalno slijedeći događaji predstavljaju sigurnosne događaje koji moraju biti zapisani:

* prijava/odjava na Rješenje (lokalni ili udaljeni pristup) – uspješna i neuspješna,
* uspješan i neuspješan pristup podacima,
* upotreba privilegiranih korisničkih imena (obrade, skripte, masovne izmjene podataka),
* nemogućnost uspostavljanja privilegiranog pristupa,
* kreiranje, brisanje i blokiranje korisničkih imena,
* izmjena korisničkih ili administratorskih prava ili dozvola,
* narušavanje prava pristupa,
* prihvaćanje ili odbijanje mrežnog pristupa,
* pristup servisima,
* startanje / zaustavljanje servisa / servera,
* izmjene konfiguracije, implementacija nadogradnji / zakrpa,
* brisanje zapisa sa sustava,
* ažuriranje sustava i/ili stavljanje zakrpi,
* detekcija malicioznih kodova i sl.

Kako bi se osigurao integritet zapisa, administratori sustava ne smiju imati prava za brisanje ili deaktivaciju zapisa vlastitih aktivnosti.

## Usluge implementacije i održavanja sustava

### Radovi i rokovi implementacije sustava

Od isporučitelja se očekuju radovi isporuke, implementacije i prilagodbe do pune funkcionalnosti sustava i puštanja u rad.

Isporučitelj mora u periodu implementacije osigurati telefonsku i e-mail podršku svakog radnog dana s vremenom reakcije unutar 2 sata, za članove projektnog tima u CARNET-u.

Od isporučitelja se očekuje minimalno 8000 čovjek-sati angažmana za izradu novih funkcionalnosti i doradu postojećih, prema definiranim zahtjevima.

Rok za isporuku gotove aplikacije do stupnja kada ona mora u potpunosti ući u sustav je osam mjeseci.

### Radovi održavanja sustava

Produkcijski sloj podrške podrazumijeva održavanje gotove aplikacije u produkcijskoj i testnoj okolini na poslužiteljima CARNET-a. Isporučitelj se mora obavezati na davanje podrške za ispravan rad isporučenog koda i aplikacije u razdoblju od pet godina od isporuke gotove aplikacije, od čega 12 mjeseci u garantnom roku.

Održavanje aplikacijskog sustava uključuje ažurnost aplikacijske infrastrukture, pravovremeno osiguravanje svih sigurnosnih i drugih zakrpi.

Isporučitelj mora registrirati četiri kategorije prijave problema u produkcijskom sloju podrške:

1. Sigurnosni problemi - problemi koji uzrokuju eskalaciju privilegija na sustavu čime ugrožavaju integritet operativnog sustava i/ili privatnost korisničkih podataka, te kritični problemi u funkcionalnosti CMS-a - problemi koji uzrokuju nedostupnost jednog ili više webova škola
2. Problemi koji uzrokuju nemogućnost prikaza većeg dijela pojedinih stranica, ili koji uzrokuju nemogućnost uređivanja većeg dijela pojedinih stranica.
3. Manji problemi ili zahtjevi za informacijama
4. Zahtjevi za novim funkcionalnostima

Isporučitelj mora organizirati sustav za praćenje zahtjeva za podrškom putem kojeg će CARNetu biti moguće prijaviti probleme te pratiti njihovo rješavanje. Rokovi za rješavanje kategorija problema su:

1. četiri sata od prijave
2. jedan radni dan od prijave
3. neodređeno, maksimalno pri redovitoj provjeri i nadogradnji aplikacije
4. neodređeno, maksimalno pri redovitoj provjeri i nadogradnji aplikacije

Redovita provjera i nadogradnja aplikacije se mora izvršiti minimalno svako šest mjeseci ili češće.

Održavanje na strani korisnika ne smije se ograničavati na samo jednu aplikativnu platformu, tj. mora biti potpuno funkcionalan u svim korištenijim browserima (Mozilla Firefox, Internet Explorer, Opera, ...).

Isporučitelj mora osigurati pomoć u organizaciji osnovnog sloja podrške krajnjim korisnicima, koju vrši CARNET-ov helpdesk.

Isporučitelj mora osigurati pomoć i u organizaciji aplikativnog sloja podrške, tj. podršku naprednim korisnicima do razine programera dodatnih modula.

### Edukacija korisnika

Ponuđač je dužan sudjelovati u edukaciji administratora sustava, te osiguravanju podrške u uspostavljanju i održavanju sustava edukacije za korisnike sustava u digitalnoj formi tečaja unutar Learning Management sustava Naručitelja ili webinara.

## Obaveze Naručitelja

### Hardver i mrežni resursi

Naručitelj se obvezuje osigurati računalni hardver i mrežne resurse potrebne za instalaciju testnih i produkcijskih instanci svih aplikacija uključenih u cjelokupno rješenje.

Predviđeni kapacitet hardvera na razini cjelokupnog rješenja:

* CPU: 150
* Broj virtualnih poslužitelja: 50
* RAM: 512 GB
* Disk: 2TB

Navedeni kapacitet odnosi se isključivo na aplikacijsko rješenje, dok će predviđeni resursi namijenjeni krajniim korisnicima biti dodatno osigurani od strane Naručitelja.

### Zajedničke funkcionalne komponente rješenja i postojećih sustava Naručitelja

Tehničko rješenje cjelokupnog informacijskog sustava za upravljanje resursima će se minimalno sastojati od sljedećih funkcionalnih kategorija poslužitelja:

* Kategorija Log poslužitelj
* centralno prikupljanje logova poslužitelja mail sustava, podijeljeno po kategorijama ili poslužiteljima
* visoka dostupnost središnjeg poslužitelja
* Kategorija Monitoring poslužitelj
* središnji nadzor sustava
* visoka dostupnost poslužitelja za nadzor
* Kategorija Management poslužitelj
* Središnje upravljanje mail sustavom za komponente sustava e-pošte na razinama ispod aplikacije ili nepokrivene aplikacijom (konfiguracija horizontalnih poslužitelja te integracija drugih poslužitelja s novim horizontalnim poslužiteljem i smanjenje broja horizontalnih poslužitelja)
* Automatizirano upravljanje komponentama sustava e-pošte
* Kategorija Backup
* *backup* i *restore* kritičnih komponenata mail sustava
* *backup* i *restore* pojedinih korisničkih sandučića e-pošte

Naručitelj se obvezuje osigurati navedene funkcionalne kategorije poslužitelja, podešavanje i implementaciju poslužiteljskih parametara, dok se od Ponuditelja očekuje podešavanje klijentske strane sustava.

## Očekivane aktivnosti od ponuditelja uključuju:

* Tehničko rješenje novog sustava uključujući dizajn, arhitekturu i dokaz rada koncepta sustava.
* Demonstraciju sučelja za korisnike s njegovim mogućnostima
* Demonstraciju administracijskog sučelja i njegovih funkcionalnosti
* Mjerenja i zatim procjenu hardverskih zahtjeva za rad sustava u okolini naručitelja s predinstaliranim Ceph SDS-om.
* Implementaciju sustava na lokaciji Naručitelja.
* Gdje je primjenjivo, migraciju postojećih korisnika i njihovih podataka s postojećeg sustava (npr kontakte, kalendare i elektroničku poštu s minimalnim uplivom na korisnike sustava).
* Dokumentaciju za isporučeni sustav, opisane promjene i konfiguracije, te uputstva za uporabu kroz kod i dokumentaciju za upravljanje sustavom.
* L3 podršku za rad sustava te podršku u režimu 24/7s
* Jamstvo za ispravan rad aplikacija i implementiranih nadogradnji i integracija
* Instalacija svih podsustava na opremi Naručitelja
* Integracija podsustava s središnjom administratorskom aplikacijom
* Održavanje podsustava tokom trajanja ugovora
* Potrebe promjene i nadogradnje aplikacija tokom trajanja ugovora minimalno u količini dodatnih 10% radnih sati iz projekta
* Osigurati izradu i postavljanje oznaka vidljivosti na svaku navedenu stavku.
* Osigurati korisničke i administratorske upute za sve isporučene sustave.

## Programski kod i programski jezici

Za traženo Rješenje očekuje se da dobavljač osigura programski kod te da se izvorni programski kod Rješenja pohrani na Naručiteljevom repozitoriju koda. Ujedno dobavljač mora osigurati mogućnost promjene koda Rješenja prema potrebama i na zahtjev Naručitelja. Dobavljač je također dužan osigurati da se sve promjene na produkcijskoj verziji Rješenja šalju isključivo s Naručiteljevog repozitorija koda.

Postojeći CARNET-ovi resursi i informacijska infrastruktura i sustavi podržavaju razvoj informacijskih sustava u sljedećim tehnologijama – HTML, CSS Javascript, PHP. Ponuđeno rješenje, potrebne integracije i nadogradnje sustava trebaju biti kompatibilna s navedenim tehnologijama i na način da Naručitelj ne mora mijenjati postojeću informacijsku infrastrukturu i sustave.

### Alat za upravljanje izvornim kodom (engl. *Source Code Management, SCM*)

Kao što je prethodno naznačeno, sve promjene na produkcijskoj verziji Rješenja potrebno je provoditi i unositi na Naručiteljevom repozitoriju koda, odnosno unutar SCM alata kojeg će osigurati Naručitelj.

SCM alat služi za upravljanje verzijama izvornog koda. SCM alat svakom programeru nudi lokalnu kopiju čitave povijesti razvoja. Omogućava korisnicima da rade istovremeno na istom projektu, bez ometanja tuđeg rada. Kad određeni korisnik završi sa svojim dijelom koda, prenese (engl. push) promjene u repozitorij koda i te se promjene ažuriraju u lokalnoj kopiji svakog drugog udaljenog korisnika koji preuzme (engl. *pull*) najnoviju kopiju projekta.

Dodatne karakteristike SCM alata Naručitelja su minimalni sljedeće:

* besplatan *open source* alat,
* kompatibilan je s više operativnih sustava, kao i sa nekim drugim SCM alatima,
* podržava brzo grananje (engl. *branching*) i spajanje te uključuje posebne alate za vizualizaciju i kretanje po nelinearnoj povijesti razvoja,
* svi podaci povezani s projektom su pohranjeni u lokalnom repozitoriju procesom kloniranja,
* svi zapisi radnji na lokalnoj kopiji programera su evidentirani i sl.

### Alat za kontinuiranu integraciju (engl. *Continuous Integration, CI*)

Svaka promjena koja se dodaje na repozitorij koda potencijalno može narušiti stabilnost Rješenja i time onemogućiti ostalim programerima u timu da nesmetano razvijaju svoje funkcionalnosti.

CI se svodi na svakodnevnu praksu da programeri automatizirano integriraju svoje promjene na repozitorij koda, pri čemu se svi problemi mogu detektirati nakon prijenosa promjena na repozitorij koda, a ne tek kad se promjene unesu na produkcijsku verziju Rješenja. Provjera ispravnosti novih promjena provodi se pomoću unit i integration testova koje programeri moraju pisati paralelno s razvijanjem funkcionalnosti aplikacije. Testovi se obavljaju nad „in-memory“ bazom podataka koja se nalazi u memoriji samo u fazi izvođenja testova, a nakon njihovog završetka briše se iz memorije. Nova verzija (engl. *build*) aplikacije se isporučuje samo u slučaju kad svi testovi „prolaze“, a u suprotnom se obavještavaju svi članovi tima o razlogu „pada“ nekog od testova što ujedno i onemogućava kreiranje nove verzije Rješenja.

Svaki programer prije nego što prenese svoje promjene na repozitorij koda, lokalno treba pokrenuti sve testove i time dobiti povratnu informaciju hoće li njegove promjene „srušiti build“. Ako programer ne pokrene lokalno testove i svejedno prenese promjene na repozitorij koda, alat za kontinuiranu integraciju Naručitelja automatski pokreće sve testove čim detektira ulazne promjene na repozitoriju koda te obavještava sve programere u timu ako je build postao nestabilan ili je build proces završio pogreškom.

## Mikroservisna arhitektura

Rješenje mora biti moguće brzo mijenjati, nadograđivati, održavati i skalirati prema potrebama poslovanja s ciljem da stabilni sustav, s novim funkcionalnostima može biti puštena u rad svaki dan.

Upravo mikroservisi omogućuju takvo funkcioniranje Rješenja. Mikroservis je nezavisno isporučiva komponenta vezanog područja koji podržava interoperabilnost putem komunikacije porukama. Mikroservisna arhitektura je stil programskog inženjerstva u kojem su visoko automatizirani i nadogradivi softverski sustavi sastavljeni od podjednako sposobnih mikroservisa. Ključna obilježja koja opisuju mikroservise su sljedeća:

* male veličine (termin „mikro“ ne odnosni se nužno na veličinu servisa u pogledu linija koda, već na njegovu funkcionalnost - svaki mikroservis slijedi princip jedne odgovornosti (engl. *Single Responsibility Principle*)),
* komunikacija porukama (komunikacija između mikroservisa najčešće se realizira putem HTTP protokola, koristeći RESTful API sučelja),
* vezani kontekstom (mikroservisi su visoko kohezivni te rade zajedno u sklopu jednog sustava),
* samostalan razvoj (svaki mikroservis se može razvijati neovisno o ostalima) te
* nezavisna isporuka (svaki mikroservis se može isporučiti neovisno o ostalima).

Svi mikroservisi Rješenja moraju biti izolirana okruženja (koja uključuju svoje binarne (izvrše) datoteke i biblioteke), unutar jednog domaćeg operativnog sustava (engl. *host*), kako je prikazano na slici u nastavku.

Slika 2: Mikroservisna arhitektura Rješenja

### Sustav za kontejnerizaciju

Kako bi se postigla željena mikroservisna arhitektura (kako je opisano u prethodnom odjeljku) potrebno je koristiti kontejnere.

Sve datoteke potrebne za pokretanje mikroservisa sadržane su u kontejneru. Kontejner može imati zasebna mrežna sučelja koja se mogu razlikovati od onih na *host-u* što bi inače moglo dovesti do konflikata pri korištenju pojedinih brojeva portova.

Potrebno je koristiti alat dizajniran za kreiranje, implementaciju i pokretanje kontejniziranih mikroservisa.

Navedeni alat mora zadovoljavati sljedeće uvjete:

* mogućnost implementacije (engl. *deployment*)lokalno, hibridno ili na oblaku,
* mogućnost limitiranja resursa kontejnera,
* podrška za više programskih jezika,
* *open source* alat,
* mogućnost automatskog ili ručnog skaliranja spremljenih kontejniziranih mikroservisa,
* integrirani set alata za samoposluživanje programera (npr. Jenkis Pipeline)
* integrirani *logging*,
* integrirani sigurnosni alati i sl.

### Operativni sustav

Rješenje mora podržavati mogućnost implementacije na *open source* operativnom sustavu (npr. Debian, Ubuntu).

### Infrastruktura

Rješenje je potrebno u potpunosti primijeniti u okolini Naručitelja (engl. *On-Premise*). Rješenje je potrebno realizirati s posebnim naglaskom na pouzdanost, skalabilnost, visoku dostupnost i sigurnost.

Naručitelj će za potrebe Rješenja osigurati testnu i produkcijsku kontejner platformu.

## Vlasništvo nad izvornim kodom i korisnička dokumentacija

Vlasništvo nad izvornim kodom te pripadajućom razvojnom, tehničkom i korisničkom dokumentacijom dobavljač je obvezan, nakon uspješne primopredaje sustava sa svim traženim funkcionalnostima, prenijeti na Naručitelja te mu predati u posjed izvorni kod programskog rješenja i sve potrebne programske biblioteke programske platforme za dalji razvoj isporučenih aplikacija u strojnom kodu i pripadajuću dokumentaciju i time prenijeti na Naručitelja pravo modifikacije i daljnjega razvoja programskog rješenja.

Naručitelj može koristiti izvorni kod programskog rješenja i programsku platformu za razvoj drugih aplikacija. Dobavljač zadržava pravo daljeg korištenja izvornog koda te ima pravo isti koristiti za dalji razvoj vlastitog rješenja.

Dobavljač je obavezan predati Naručitelju korisničku dokumentaciju koja uključuje:

* funkcionalnosti sustava - popis ključnih funkcionalnosti i namjena (opis funkcionalnosti)
* nefunkcionalni opis sustava - računalna platforma (klijentska razina, poslužiteljska razina), performanse i raspoloživost, sigurnost, komunikacija s vanjskim sustavima, dizajn sučelja i slično
* arhitekturu sustava i opis modela podataka - aplikativna arhitektura sustava (platforma, klijentska razina - prezentacijski i servisni sloj, poslužiteljska razina - servisni i podatkovni sloj), izvedbena arhitektura sustava (servisni i podatkovni sloj - broj poslužitelja, VM, fizički poslužitelji, zaštita sustava, međusobna povezanost,...), okoline i instance sustava (razvojna, testna i produkcijska okolina)
* korištene tehnologije i razvojni alati - popis tehnologija i alata, te vrsta i namjena
* upute za administratore sustava
* upute za korisnike - upute za različite uloge korisnika

## Komunikacija na projektu i nadzor provedbe ugovora

Naručitelj će kontinuirano pratiti provedbu ugovorene usluge te je stoga odabrani dobavljač dužan omogućiti Naručitelju pravovremeni i redoviti uvid u sve aktivnosti koje će se provoditi po ugovoru sklopljenom na temelju ovog procesa javne nabave. Nadalje, odabrani dobavljač treba Naručitelju omogućiti neposredan uvid u rad stručnjaka i rezultate u svakom trenutku provedbe ugovorenih usluga.

Naručitelj će za potrebe razvoja sadržaja i praćenja napretka provedbe osigurati potrebnu računalnu infrastrukturu za produkcijsku i testnu okolinu, koja će dobavljaču omogućiti redovno dostavljanje sadržaja u razvoju, odnosno programskog koda u repozitorij koda i u odgovarajuću okolinu.

Naručitelj će osigurati i zahtijevati propisani kanal komunikacije (odnosi se na alat za upravljanje zadacima) između tehničkih osoba radi preuzimanja zahtjeva za izmjenama i ispravcima uočenih grešaka ili nedostataka u izrađenom sadržaju.

Praćenje napretka provedbe od strane Naručitelja odvija se putem redovitog izvještavanja od strane voditelja projekta, putem redovitih status sastanaka, minimalno jednom u dva tjedna tokom implementacije rješenja.

Neposrednim uvidom u rad stručnjaka i rezultate u svakom trenutku provedbe ugovorenih usluga, Naručitelj će pratiti napredak provedbe ugovora.

Po uvidu Naručitelja u rad odabranog dobavljača, Naručitelj ima pravo dati komentare na rad i rezultate odabranog dobavljača. Odabrani dobavljač dužan je usvojiti komentare u postavljenom roku definiranom u skladu s dogovorom s Naručiteljem.

## Sigurnost informacijskog sustava za upravljanje resursima CARNET omega

### Sigurnost po dizajnu

Ponuditelj treba osigurati da je sustav i svi njegovi elementi u skladu s najboljom sigurnosnom praksom, tako da štiti sebe i informacije koje obrađuje te pruža otpor napadačima.

Ako prilagodbe sustava za potrebe naručitelja budu uključivale integraciju ili povezivanje s drugim naručiteljevim sustavima ili uslugama, one također moraju biti izrađene u skladu s najboljom sigurnosnom praksom, prema principima sigurnosnog programiranja i takve da je sigurnost ugrađena u njih od samog dizajna sustava.

### Sigurnosno testiranje sustava

Nakon izrade svih funkcionalnosti sustava, a prije stavljanja u produkcijsko okruženje odabrani ponuditelj dužan je omogućiti naručitelju provođenje sigurnosnog testiranja. Postupak sigurnosnog testiranja podrazumijeva detekciju eventualnih sigurnosnih propusta u sustavu automatiziranom analizom korištenjem specijaliziranih alata te ručne provjere sigurnosti. Opseg sigurnosnog testiranja opisan je u Poglavlju: “Opseg sigurnosnog testiranja sustava”.

U svrhu sigurnosnog testiranja potencijalni ponuditelj je dužan:

1. Na infrastrukturi naručitelja u dijelu u kojem raspolaže administratorskim ovlastima, omogućiti testnu okolinu koja  treba biti identična produkcijskoj (pri čemu verzija sustava treba biti sukladna onoj koja će se koristiti u produkciji) s „root“ (administratorskim) pristupom na sustav
2. Osigurati korisničke račune za sve uloge koje postoje u sustavu
3. Osigurati pristup produkcijskom sustavu kako bi mogla biti izvršena provjera konfiguracija i implementacije sustava s „root“ (administratorskim) pristupom
4. Osigurati mogućnost sigurnosne provjere izvornog koda sustava
5. Dostaviti izvorni kod prilagodbi sustava za potrebe naručitelja ako one podrazumijevaju integraciju ili povezivanje s drugim naručiteljevim sustavima ili uslugama
6. Dostaviti ažurnu tehničku dokumentaciju prilagodbi sustava za potrebe naručitelja ako one podrazumijevaju integraciju ili povezivanje s drugim naručiteljevim sustavima ili uslugama.

Sigurnosno testiranje obavljat će naručitelj, a odabrani ponuditelj dužan je omogućiti provođenje testiranja od strane naručitelja. Odabrani ponuditelj obvezan je otkloniti eventualne sigurnosne propuste sukladno rezultatima testiranja.

Postupak sigurnosnog ispitivanja podrazumijeva detekciju eventualnih sigurnosnih propusta u aplikaciji automatiziranom analizom korištenjem specijaliziranih alata te ručne provjere sigurnosti.

Osim prije inicijalnog postavljanja sustava u produkcijsku okolinu, testiranje će se provoditi: periodički (najviše jednom godišnje za vrijeme trajanja ugovora) te izvanredno (na zahtjev naručitelja, u slučaju veće nadogradnje sustava ili u slučaju sigurnosnog incidenta).

### Uklanjanje uočenih sigurnosnih propusta

Razvijeni programski sustav se ne smije staviti u produkciju ako nisu ispravljeni pronađeni propusti označeni kao kritični ili srednji.

U slučaju periodičkih ili izvanrednih sigurnosnih testiranja potencijalni ponuditelj je dužan ispraviti uočene sigurnosne propuste prema rokovima definiranima Tablicom: Odabrani ponuditelj će o svom trošku u sklopu poslova održavanja, raditi sigurnosne ispravke sukladno zahtjevu i u roku dogovorenim s naručiteljem.

Rokovi za uklanjanje sigurnosnih propusta:

|  |  |
| --- | --- |
| **Razina kritičnosti sigurnosnog propusta** | **Rok za uklanjanje sigurnosnog propusta** |
| Sigurnosni propusti kritične razine  | do 3 dana od zaprimanja rezultata testiranja  |
| Sigurnosni propusti srednje razine  | do 7 dana od zaprimanja rezultata testiranja  |
| Sigurnosni propusti niske razine  | do 30 dana od zaprimanja rezultata testiranja  |

Sigurnosne ranjivosti kritične razine rizika predstavljaju najveću opasnost za sustav i uglavnom se odnose na greške u kodu, odnosno na zastarjele programske pakete i operacijske sustave za koje više ne postoji podrška proizvođača odnosno za zastarjele inačice kojima je potrebna hitna nadogradnja. Za kritične ranjivosti najčešće postoje javno objavljeni alati i upute kako iskorištavanjem takve ranjivosti napadač može u potpunosti preuzeti kontrolu nad cijelim sustavom.

Sigurnosne ranjivosti srednje razine rizika predstavljaju ranjivosti nešto niže razine sigurnosnog rizika, ali su također prilično velika prijetnja ako se ne provedu odgovarajuće mjere zaštite. Za iskorištavanje ranjivosti napadač mora posjedovati određena znanja i vještine pa se tako npr. može ubaciti u komunikaciju između korisnika i poslužitelja i saznati osjetljive podatke kao što su korisnička imena i lozinke, što se kasnije može iskoristiti za daljnje napade na sustav.

Sigurnosne ranjivosti niskog rizika predstavljaju propuste koji uključuju otkrivene servise koji se mogu iskoristiti za otkrivanje sporednih informacija o sustavu. Iako ove ranjivosti pripadaju kategoriji ranjivosti s najnižom razinom rizika, preporučujemo i njihovo otklanjanje. Potencijalni napadač može iskoristiti ovako prikupljene informacije za daljnje planiranje napada na sustav.

### Opseg sigurnosnog testiranja sustava

Elementi provjere sigurnosti su:

* Udaljeno ispitivanje poslužitelja
	+ Udaljeno ispitivanje poslužitelja podrazumijeva da se tijekom ispitivanja ne pristupa poslužitelju korištenjem korisničkog računa već se udaljeno utvrđuje postojanje aktivnih servisa na poslužitelju te provjerava postojanje sigurnosnih ranjivosti u njima.
	+ Za provođenje ispitivanja potrebno je omogućiti mrežnu dostupnost poslužitelja s IP adresa s kojih će se provoditi ispitivanje.
* Lokalno ispitivanje poslužitelja (administratorski i limitirani korisnički računi)
	+ Ispitivanje poslužitelja se provodi korištenjem lokalnog korisničkog računa na poslužitelju. Ispitivanja se provode s limitiranim i s administratorskim ovlastima kako bi se dobio sveobuhvatan uvid u sigurnost poslužitelja. Ispituje se mogućnost izvođenja aktivnosti koje mogu imati neplanirani utjecaj na aplikaciju korištenjem limitiranog korisničkog računa, a korištenjem administratorskog računa ispituju se konfiguracijske postavke poslužitelja, procesi bitni za rad aplikacije, postavke aplikacije, ovlasti procesa aplikacije, zaštita poslužitelja.
	+ U sklopu lokalnog ispitivanja po potrebi se ispituje postojanje slabih korisničkih lozinki. Slabim lozinkama smatraju se lozinke koje su kraće od 8 znakova, lozinke koje predstavljaju riječi iz rječnika, sadrže samo mala ili velika slova ili samo brojeve, ne sadrže specijalne znakove, predstavljaju često korištene lozinke ili sadrže pripadajuća korisnička imena. Obilježja slabih lozinki se mogu proširiti u slučaju pojave novih elemenata koji čine slabe lozinke.
* Udaljeno ispitivanje aplikacije
	+ Udaljeno ispitivanje aplikacije obuhvaća ispitivanje aplikacije iz korisničkog pogleda s ciljem detektiranja mogućnosti izvođenja neovlaštenih korisničkih aktivnosti. Ovo ispitivanje podrazumijeva korištenje skenera te izvođenje ručnih provjera.
* Lokalno ispitivanje samostalno razvijene aplikacije
	+ Ispitivanje obuhvaća ispitivanja navedena u točki 3. uz ispitivanje izvornog koda aplikacija koji je samostalno razvijen i vanjskih gotovih modula ako se koriste. Ispitivanje obuhvaća i ispitivanje konfiguracijskih postavki aplikacije.

# Prilog A

## Postojeći sustavi

CARNET trenutno svim osnovnim i srednjim školama, njihovim zaposlenicima, nastavnicima i učenicima otvara korisnički elektronički identitet i adresu e-pošte u postojećoj usluzi *hostinga* za srednje i osnovne škole (HUSO).

Opisane funkcionalnosti postojećih sustava potrebno je replicirati u CARNET omega sustavu, osim ako nije drugačije opasano u funkcionalnim zahtjevima iz prethodnih poglavlja.

Imenički servis HUSO sustava je dio AAI@EduHr sustava, što ga čini jednim od ključnih infrastrukturnih servisa za autentikaciju na brojne usluge.

Više detalja o postojećim sustavima na poveznicama:

* <https://www.carnet.hr/usluga/web-za-skole/>
* <https://www.carnet.hr/usluga/hosting-usluga-za-skole/>
* <https://www.aaiedu.hr/o-sustavu/sto-je-aaieduhr>

Uz korisničke identiteta, adrese i sandučiće e-pošte u protekla dva desetljeća, za različite svrhe i namjene uspostavljene su brojne usluge kojima je svrha bilo udomljavanja mrežnih (web) stranica korisnika sustava.

* Školama je kroz HUSO sustav omogućena izrada web stranica putem CARNET-ovog sustava za upravljanje sadržajem, odnosno posluživanje statičkih web stranica.
* CARNET-ov Javni poslužitelj je računalni sustav putem kojeg veći broj pojedinaca, zaposlenih u različitim ustanovama, odnosno zaposlenih u ustanovama izvan sustava Ministarstva znanosti i obrazovanja za osobne, nekomercijalne potrebe koristi mrežne usluge i mrežne informacijske servise CARNET-a i druge resurse dostupne putem elektroničkog identiteta u sustavu AAI@EduHr. Na Javnom poslužitelju se također nalaze i brojni gostujući informacijski servisi koji doprinose unapređenju informacijskog prostora Republike Hrvatske.
* Uslugom 3u1 korisnicima from.hr domena omogućuje se jednostavna izrada web stranice u WordPress sustavu.
* Nestandardni hosting obuhvaća udomljavanja mrežnih stranica od posebne važnosti.

Hosting usluga za srednje i osnovne škole sastoji se od niza komponenata i podsustava, koje su implementirane kroz sustave visoke dostupnosti:

* aplikacija za unos elektroničkih identiteta i upravljanje uslugama (trenutno na adresi <http://admin.skole.hr> )
* podsustav za integraciju hosting sustava sa sustavom eMatice <https://www.carnet.hr/projekt/e-matica/> (unutar <http://admin.skole.hr>)
* AAI@EduHr imenički podsustav
	+ servisi LDAP, RADIUS, AOSI
	+ 650.000 korisnika
* Podsustav e-pošte
	+ IMAP, POP, SMTP, aliasi, antispam, antivirus, webmail
	+ 650.000 korisnika, 9TB podataka
* DNS podsustav
	+ upravljanje zonama i zapisima za približno 2000 ustanova
* web podsustav za CARNET-ov CMS za škole (Strix)
	+ preko 1200 ustanova
	+ ukupno 3.5 TB podataka
* web hosting podsustav za vlastite sadržaja škola (static web)

Od 1. ožujka 2007. godine CARNET je osnovnim i srednjim školama omogućio korištenje CMS-a u sklopu HUSO-a, koji je razvijen i dizajniran posebno za potrebe škola. Sustav je realiziran u suradnji sa vanjskim dobavljačem, te je nakon nekoliko godina razvoj i održavanje preuzeo CARNET. Trenutno je u sustavu više od 1.200 škola, a koristi ga i veći broj raznih udruga i projekata povezanih sa školama, koje su uz posebno odobrenje CARNET-a dobile sustav na korištenje. Postojeći sustav se temelji na Strix portalu, a za njegovo korištenje škola mora imati aktiviran HUSO korisnički račun. Web stranice se aktiviraju kroz aplikaciju za administraciju HUSO korisničkih računa na <https://admin.skole.hr>. Upute za korisnike za CMS sustav se nalaze na <https://www.carnet.hr/wp-content/uploads/2019/11/CMS-upute_2019.pdf> .

Svaka škola može odlučiti želi li koristiti CARNET-ov CMS za škole, kada će dobit će na izbor više gotovih dizajna i predložaka te niz funkcionalnosti i kolaboracijskih alata (vijesti, forumi, ankete, html editor, RSS i dr.). Odabirom CMS-a omogućeno je efikasno izrada i održavanje sadržaja mrežnih stranica škola, bez potrebe za kompleksnim i tehničkim znanjima. Cilj je uspostaviti jedinstveni CMS sustav za sve škole koji je osnova za samostalno održavanje web stranica od strane ovlaštenih školskim administratora.

## Sustav za upravljanje elektroničkim identitetima korisnika

Sustav imeničke infrastrukture CARNET alfa izdvojeni je sustav koji sadrži identitete korisnika i ustanova a zajedno sa sustavom CARNET omega čine okosnicu CARNETovih sustava. Sama izvedba sustava CARNET alfa nije u opsegu ove nabave, ali s obzirom na nužnu integraciju koju je potrebno realizirati sastavni je dio ove dokumentacije.

CARNET alfa je sustav koji se temelji na LDAP imeničkoj infrastrukturi i nužno je usklađen s AAI@EduHr imeničkim sustavom. Imenička struktura definirana je AAI@EduHr imeničkim shemama (hrEduPerson i hrEduOrg) i sadrži sve ključne (matične) podatke CARNET-ovih korisnika i ustanova članica iz sustava osnovnoškolskog i srednjoškolskog obrazovanja u Republici Hrvatskoj.

Sustav CARNET alfa je jedan od ključnih infrastrukturnih servisa za autorizaciju i autentikaciju na brojne usluge, odnosno sustav koji upravlja identitetom i pristupom (IAM, engl. Identity and Access Management). Sastoji se od tri ključne funkcionalnosti:

* upravljanje identitetom korisnika u smislu definiranja i upravljanje ulogama i pristupnim pravima korisnika
* mogućnost korištenja više-stupanjske autentikacije za prijavu korisnika kao sigurnosna komponenta
* mogućnost korištenja drugih aplikacija bez potrebe za ponovnim unosom korisničkog imena i lozinke, SSO prijava (SSO, engl. Single Sign-On)

Detaljna dokumentacija AAI@EduHr sustava nalazi se na <https://www.aaiedu.hr/> .

1. Sustav HUSO za potrebe razumijevanja predmeta nabave je opisan u prilogu A. [↑](#footnote-ref-2)
2. Opis ustava CARNET alfa nalazi se u poglavlju „Sustav za upravljanje elektroničkim identitetima korisnika“ [↑](#footnote-ref-3)
3. „identifikator-ustanove“ je jedinstveni identifikator za ustanovu u kojoj je korisniku otvoren elektronički identitet. [↑](#footnote-ref-4)
4. Informacije o postojećem sustavu za upravljanje sadržajem (CMS) navedene su prilogu "3. Prilog A" u poglavlju "3.1. Postojeći sustavi" [↑](#footnote-ref-5)