

Predmet nabave:

Nadogradnja aplikacije za digitalni potpis

**TEHNIČKA SPECIFIKACIJA**

## Sadržaj

Uvod .....	3
Tražene nadogradnje.....	3
SignumID e-Platforma za visokoškolske ustanove .....	3
SignumID e-Potpis modul: .....	4
Podrška za korištenje certifikata za digitalni pečat .....	5
Podrška za korištenje udaljenih certifikata za digitalni pečat .....	5
Jamstveni rok.....	5
Adaptivno održavanje .....	7
Infrastrukturna okolina Naručitelja .....	8
Rok izvođenja usluge.....	8
Obaveze naručitelja .....	9
Sigurnosno testiranje aplikacije .....	9
Komunikacija.....	10
Plaćanje .....	10

## Uvod

CARNET u redovnom internom poslovanju, kao i poslovanju s korisnicima iz sustava školstva, koristi aplikaciju za digitalni potpis na adresi potpis.carnet.hr

Aplikacija je web bazirano rješenje razvijeno nad Microsoft .Net Core uz korištenje PostgreSQL baze podataka. Povezano je na interne CARNET sustave LDAP i e-mail te AAI@EduHr autentikacijsku i autorizacijsku infrastrukturu sustava znanosti i visokog obrazovanja. Za komunikaciju kriptouređaja na lokalnom web sučelju korisnika koriste se middleware komponente koje podržavaju eID, kID, FINA tokene i pametne kartice.

Predmet nabave je nadogradnja aplikacije za digitalni potpis u CARNET-u za ustanove iz sustava visokog školstva:

- SignumID e-Platforma za ustanove iz sustava visokog školstva
- SignumID e-Potpis modul za ustanove iz sustava visokog školstva
- Podrška za korištenje certifikata za digitalni pečat
- Podrška za korištenje udaljenih certifikata za digitalni pečat

za razdoblje od potpisa ugovora do kraja projekta e-Sveučilišta. Jamstveni rok uključuje usluge preventivnog i korektivnog sukladno detaljnom opisu navedenom u poglavlju "Tražene vrste održavanja sustava". Adaptivno održavanje uključuje razvoj i implementaciju novih ili promjene u postojećim funkcionalnostima.

## Tražene nadogradnje

### SignumID e-Platforma za visokoškolske ustanove

- Omogućiti korištenje platforme za svaku visokoškolsku ustanovu u Republici Hrvatskoj i Ministarstvo znanosti i obrazovanja
  - Multitenant rješenje, djelatnici svake ustanove trebaju moći pristupiti dokumentima svoje ustanove
    - Korisnici zaposleni na više ustanova mogu odabrati prilikom prijave za koju se ustanovu prijavljuju
    - Sustav prepoznaje hijerarhiju ustanova (MZO -> Sveučilište -> Sastavnica sveučilišta)
      - Podatke o ustrojstvu hijerarhije ustanova unosi i održava Naručitelj
  - Po jedna odgovorna osoba iz svake ustanove ima ovlasti administrirati dokumentima svoje ustanove te može te ovlasti dodijeliti ostalim osobama na svojoj ustanovi
    - Dodavanje obrazaca, dodavanje obilježja dokumenata
  - Ustanove mogu međusobno razmjenjivati dokumente

- Dodatna instanca platforme na kojoj će ustanove međusobno izmjenjivati dokumente
- Prijava u sustav moguća je putem AAI@EduHr korisničkog računa ili s potpisnim certifikatom
  - Sustav AAI@EduHr je autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Svaka ustanova iz sustava Ministarstva znanosti i obrazovanja koja je uključena u sustav AAI@EduHr ima vlastitu bazu (tzv. LDAP imenik) u kojoj su pohranjeni elektronički identiteti korisnika iz te ustanove
  - Po uključenju ustanove u sustav, sustav se spaja na LDAP imenik ustanove i dohvaća podatke o djelatnicima
- Učitani dokumenti zadržavaju se u aplikaciji dvije godine nakon čega se brišu
- Sustav treba omogućiti masovno preuzimanje svih odabranih dokumenata
- Korisnicima u sustavu trebaju biti dostupne korisničke upute
- Mogućnost pretraživanja dokumenata na ustanovi
  - Prilikom pretraživanja moguće je odabrati više od jednog obilježja dokumenata
- Korisnici mogu pokrenuti novi proces ovjere dokumenta
- Korisnici mogu pokrenuti novi proces razmjene dokumenta
- Korisnici mogu pokrenuti provjeru certifikata na dokumentu
- Korisnici mogu ispunjavati učitane obrasce
- Korisnici mogu pregledati svoje dokumente i dokumente na svojoj ustanovi
  - Dokumenti su razvrstani prema statusu (u ovjeri, odobriti, potpisati, odbijeni)
- U pregledu dokumenata moguće je masovno dodati obilježja označenim dokumentima
- U pregledu dokumenata moguće je masovno dodati osobe u potpisni tijek označnim dokumentima
- Na popisu svih dokumenata prikazan je datum kreiranja pojedinog dokumenta
- Korisnici dobivaju obavijesti kada trebaju pristupiti dokumentu
- Korisnici mogu pretraživati druge korisnike svoje ustanove
  - Korisnici iz nadređenih ustanova mogu pretraživati sve korisnike podređenih ustanova
  - Korisnici se mogu pretražiti po e-mail adresi, tipu korisnika i ustanovi
- Korisnici mogu pregledati osobne informacije na svom profilu
  - Na profilu je dostupan podatak o isteku valjanosti certifikata korisnika prema podacima iz RA aplikacije ili s pametne kartice

### SignumID e-Potpis modul:

- Za svaku visokoškolsku ustanovu u Republici Hrvatskoj i Ministarstvo znanosti i obrazovanja koje koriste SignumID e-Platformu potrebno je omogućiti korištenje SignumID e-Potpis modula.
- Kod potpisivanja nije bitan redoslijed kojim potpisnici potpisuju dokument
- Korisnicima koji su dodani u tijek potpisivanja potrebno je dodati obavijest
- Na pregledu dokumenta prikazuju se datum i vrijeme svake akcije (odobrenje, potpis)

## Podrška za korištenje certifikata za digitalni pečat

- U okviru potpisnog modula potrebno je omogućiti odobravanje, potpisivanje i pečatiranje dokumenata digitalnim pečatom.

## Podrška za korištenje udaljenih certifikata za digitalni pečat

- U okviru potpisnog modula potrebno je omogućiti pečatiranje i potpisivanje dokumenata udaljenim certifikatom za digitalni pečat i digitalni potpis.

## Jamstveni rok

Jamstveni rok traženih nadogradnji uključuje:

### 1. Preventivno održavanje

Praćenje redovitog rada aplikativnih sustava. Isporučitelj će kontinuirano provjeravati rad aplikacijskih sustava kako bi se preventivno mogle obaviti sve potrebne akcije nužne za optimalan i ispravan rad aplikacijskih sustava. Preventivno održavanje obavlja se samo radnim danom sukladno planu i uputama Isporučitelja o održavanju aplikacijskih sustava kojeg odobrava Naručitelj.

Preventivno održavanje obuhvaća:

- osiguranje novih verzija aplikativnih komponenti sustava
- testiranje novih verzija aplikativnih komponenti sustava u testnom laboratoriju Isporučitelja
- testiranje novih verzija aplikativnih komponenti sustava na aktualnim verzijama operacijskog sustava, baze podataka i razvojnih alata
- osiguravanje novih zakrpa (fix) za komponente aplikativnog sustava
- testiranje novih zakrpa (fix) za komponente aplikativnog sustava
- provjeru i optimizaciju performansi sustava: performanse upita i aplikativnih procedura

### 2. Korektivno održavanje

Otklanjanje uzroka zastoja u radu aplikativnih sustava, a Isporučitelj ga obavlja po prijavi zastoja ili neispravnosti u radu od strane Naručitelja:

- ispravke aplikativnih grešaka koje su se dogodile unutar postojećih funkcionalnosti i programskog koda
- optimizacije PostgreSQL upita obuhvaćenih korištenim modelom podataka zbog otklanjanja problema u radu sustava
- korektivne intervencije na komponentama sustava primjenom zakrpa (fix) ili nadogradnjom (upgrade) na novu verziju softvera
- korektivne intervencije vezane za konfiguracijske parametre komponenti sustava
- korektivne intervencije u slučajevima kada aplikacije ne rade prema zadanoj specifikaciji na način da otkrije uzrok problema, a započete poslove privede kraju

- testiranje novih verzija softvera (aplikativnih komponenti sustava) u okruženju Korisnika
- osiguravanje novih zakrpa (fix) za komponente aplikativnog sustava
- testiranje novih zakrpa (fix) za komponente aplikativnog sustava u okruženju Korisnika
- prilagodbe pri nadogradnji operativnog sustava i programskih paketa na poslužiteljima Korisnika (nadogradnje radi Korisnik)

Procedura kod obavljanja korektivnog održavanja uključuje sljedeće korake:

- prijava greške (Naručitelj) u sustav za prijavu grešaka Isporučitelja
- pronalaženje greške (Isporučitelj)
- ispravak greške (Isporučitelj)
- testiranje (Isporučitelj, Naručitelj)
- prihvaćanje testa (Isporučitelj)
- instalacija promjene u "produkcijsku"

Poteškoće u radu sustava naručitelj prijavljuje putem sustava za prijavu grešaka kojeg osigurava izvršitelj. Sustav omogućuje:

- prijavu poteškoća
- pregledavanje prijašnjih prijava
- pretraživanje prijašnjih prijava
  - po ključnim riječima
  - po broju prijave
  - po kategorijama
  - po statusu (otvoren, zatvoren)
- promjenu statusa prijave
- promjenu prioriteta prijave
- ponovno otvaranje zatvorene prijave
- uvid u prijave drugih korisnika u ustanovi naručitelja

Isporučitelj je dužan, za vrijeme trajanja ugovora, osigurati dostupnost i raspoloživost stručnog osoblja za izvršavanje usluga koje su predmet nabave, a kako bi se planirane aktivnosti neometano i na vrijeme izvršile. Isporučitelj treba pristupiti otklanjanju prijavljenih poteškoća unutar dva sata od vremena prijave. Tijekom rješavanja poteškoća, Isporučitelj treba redovito izvještavati Naručitelja o statusu rješavanja poteškoće.

Maksimalno dopušteno vrijeme odziva iznosi:

- 4 sata za Prioritet 1,
- NBD (eng. Next Business Day, standardna oznaka za sljedeći radni dan) za Prioritet 2,
- 2NBD (označava dva radna dana) za Prioritet 3
- te 3NBD (označava 3 radna dana) za Prioritet 4.

Isporučitelj mora registrirati četiri kategorije prijave problema:

Prioritet 1

- Sigurnosni problemi - problemi koji uzrokuju eskalaciju privilegija na sustavu čime ugrožavaju integritet operativnog sustava i/ili privatnost korisničkih podataka
- Problemi u radu sustava koji uzrokuju nemogućnost rada većeg broja korisnika
- Problemi u radu sustava koji uzrokuju pogrešan rad ključnih funkcionalnosti sustava ili rad sustava u cijelosti

#### Prioritet 2

- Problemi u radu sustava koji uzrokuju nemogućnost rada manjeg broja korisnika ili grupe korisnika
- Zahtjevi za novim funkcionalnostima koje su povezane s ključnim poslovnim procesima u cjelovitom sustavu

#### Prioritet 3

- Funkcionalnosti sustava na testnim instancama sustava
- Zahtjevi za novim funkcionalnostima
- Zahtjevi koji se odnose na pojašnjenje rada poslovnih procesa u sustavu

#### Prioritet 4

- Zahtjevi za novim funkcionalnostima koje će unaprijediti korisničko iskustvo
- Zahtjevi za manje važnim novim funkcionalnostima

## Adaptivno održavanje

Adaptivno održavanje sustava odnosi se na razvoj i implementaciju novih ili promjene u postojećim funkcionalnostima, a obuhvaća sljedeće poslove:

- aplikativne izmjene - promjene i dorade postojeće funkcionalnosti ili dodavanje novih funkcionalnosti unutar postojećeg aplikativnog i sistemskog okruženja
- migracija na novi podatkovni sustav sukladno zahtjevima naručitelja
- poboljšanje performansi sustava zbog povećanog broja korisnika i/ili povećane potrebe korisnika
- unaprjeđenja korisničkog sučelja radi jednostavnijeg i bržeg obavljanja aktivnosti
- prilagođavanje aplikacijskog sustava optimalnoj razmjeni podataka s drugim aplikacijama, servisima, itd.
- tehnološke nadogradnje sustava te rad s podacima

Procedura kod obavljanja adaptivno održavanja uključuje sljedeće korake:

- prijava Zahtjeva za promjenom (Naručitelj)
- analiza i procjena zahtjeva (Isporučitelj)
- prihvatanje procjene zahtjeva (Naručitelj)
- razvoj (Isporučitelj)
- testiranje (Isporučitelj, Naručitelj)

- prihvaćanje testa (Naručitelj)
- instalacija promjene u "produkcijску" okolinu

Tijekom trajanja ugovora, Isporučitelj je dužan jednom mjesečno izvještavati Naručitelja o statusu nadogradnji te planiranim budućim nadogradnjama, u obliku sastanka.

## Infrastrukturalna okolina Naručitelja

Infrastrukturalna okolina Naručitelja na kojem je udomljen sustav uključuje virtualno okruženje sljedećih karakteristika:

Dostupne okoline	SLA PRIORITET		
	PRIORITET 1		BEST EFFORT
	PRODUKCIJA		TEST
OpenStack (KVM virtualizacija)	OSP PROD DC1	OSP PROD DC2	NIJE DOSTUPNO
Kontejnerska okolina	OKD-PROD		OKD-TEST
Garantirani uptime	98%		90%
Deployment opcije	Terraform/Cloud-init, HELM, Git		Terraform/Cloud-init, HELM, Git
Git branch	master, main, prod		test
Backup	File based backup za: NFS PV i VM		Ne

Softver

OS: Debian GNU/Linux 11

Nginx

PostgreSQL

Dobavljač je dužan predložiti arhitekturu rješenja koju naručitelj mora odobriti. Preferirani su multitenant deploymenti, cloud-native aplikacije i rješenja koja se mogu efikasno skalirati.

## Rok izvođenja usluge

Razdoblje izvođenja usluge nadogradnje je 9 mjeseci od datuma sklapanja ugovora, a jamstveni rok kraja projekta e-Sveučilišta (31.12.2025.).



## Obaveze naručitelja

Naručitelj se obvezuje da će tijekom cijelog trajanja Ugovora:

- osigurati uvjete potrebne za nesmetan rad usluge (fizički smještaj, električna energija, klimatski uvjeti, i sl.);
- osigurati povezanost usluge na CARNET mrežu i na Internet;
- omogućiti udaljen pristup s Interneta prema usluzi u svrhu administracije. Ovlaštena osoba dobavljača će pismeno ili e-mailom obavijestiti Ovlaštenu osobu Naručitelja s kojih IP adresa i korištenjem kojih sigurnih mrežnih protokola je potrebno omogućiti udaljeni pristup usluzi;
- Pripremiti poslužitelje prema dogovoru s dobavljačem (instalacija OS-a i paketa iz službenih repozitorija, podešavanje vatrozida te ako se radi o virtualnom poslužitelju postaviti broj procesora, memorije te količine diskovnog prostora)
- Osigurati korisničke račune osobama koje imenuje ovlaštena osoba dobavljača poštujući princip minimalnih privilegija;
- Periodički instalirati sigurnosne nadogradnje operacijskog sustava u dogovoru s ovlaštenom osobom dobavljača. Procedure nadogradnji i provjere rada sustava nakon istih biti će dogovorene s ovlaštenom osobom dobavljača te će biti dostavljene ovlaštenoj osobi iz CARNET-a pisanim putem;
- Osigurati nadzor kritičnih servisa na poslužitelju te osigurati dojavu nedostupnosti imenovanim osobama dobavljača;
- Osigurati periodičko sigurnosno kopiranje (eng. backup) na udaljeni medij poslužitelja podataka (datoteka i direktorija) koje definira dobavljač. U slučaju da je potrebno sigurnosno kopiranje posebnih izvora podataka (npr. baza podataka) dobavljač je dužan podatke pripremiti (eng. dump ili izvoz podataka) da iste može preuzeti softver za sigurnosno kopiranje. Periodičko brisanje starih izvezenih podataka nakon sigurnosnog kopiranja je dužnost dobavljača;

## Sigurnosno testiranje aplikacije

Naručitelj provodi sigurnosno testiranje sustava, a Izvršitelj je dužan omogućiti provođenje. Postupak sigurnosnog ispitivanja podrazumijeva detekciju eventualnih sigurnosnih propusta u aplikaciji automatiziranom analizom korištenjem specijaliziranih alata te ručne provjere sigurnosti. Izvršitelj će o svom trošku raditi sigurnosne ispravke.

Sigurnosno testiranje će se provoditi sljedećim tempom:

- Periodički (najviše jednom godišnje za vrijeme trajanja ugovora)
- Izvanredno (na zahtjev, u slučaju veće nadogradnje sustava, u slučaju sigurnosnog incidenta)

U svrhu sigurnosnog testiranja, dobavljač je na zahtjev dužan omogućiti:

- testnu okolinu identičnu produkcijskoj na kojoj će biti aplikacija puštena u rad (pri čemu verzija aplikacije mora biti sukladna onoj koja će se koristiti u produkciji) s „root“ (administratorskim) pristupom na sustav
- korisničke račune unutar aplikacije za sve uloge koje postoje u aplikaciji

- pristup produkcijskom sustavu kako bi tamo mogla biti izvršena provjera konfiguracija sustava s „root“ (administratorskim) pristupom

Sigurnosno testiranje može potrajati najviše 14 radnih dana.

Po završetku sigurnosnog testiranja Izvršitelj je dužan poduzeti sve adekvatne mjere za ispravljanje sigurnosnih propusta.

## Komunikacija

Tijekom trajanja ugovora Izvršitelj je dužan održavati sastanke s Naručiteljem na mjesečnoj bazi te prema potrebi na zahtjev Naručitelja i češće, gdje će naručitelj biti detaljno upoznat s dinamikom održavanja Sustava kao i s eventualnim poteškoćama na koje je Izvršitelj naišao u radu. Sastanci se održavaju na lokaciji Naručitelja. Komunikacija između Izvršitelja i Naručitelja će se odvijati prvenstveno putem elektroničke pošte, a po potrebi i telefonskim putem odnosno videokonferencijskim pozivima. Za potrebe provedbe održavanja Sustava bit će kreirana mailing lista na koju će se dodati svi sudionici.

## Plaćanje

Za uslugu nadogradnje sustava Naručitelj se obavezuje Izvršitelju isplatiti troškovnikom definiran iznos nakon odrađene nadogradnje. Za odrađene sate adaptivnog održavanja Naručitelj se obavezuje isplatiti troškovnikom definiran iznos na mjesečnoj bazi.

Izvršitelj je dužan na mjesečnoj bazi sastaviti izvješta o stanju sustava

Primopredajni zapisnik o izvršenoj nadogradnji treba sadržavati opis nadogradnji i poduzetih akcija, a primopredajni zapisnik o adaptivnom održavanju treba sadržavati popis poduzetih radnji u svrhu adaptivnog održavanja Sustava (opis, vrijeme, rezultat, broj utrošenih sati te broj preostalih adaptivnih sati do isteka ugovora).

Obavezne stavke mjesečnog izvještaja su:

- izvještaj o radu i stanju Sustava
- popis poduzetih radnji u svrhu preventivnog održavanja Sustava (opis, vrijeme, rezultat)
- popis poduzetih radnji u svrhu korektivnog održavanja Sustava (opis, vrijeme, rezultat)

Izvršitelj će nakon obostrano ovjerenog primopredajnog zapisnika Naručitelju ispostaviti račun za obavljene poslove navedene u primopredajnom zapisniku. Naručitelj se obavezuje plaćati Izvršitelju na temelju ispostavljenih računa, a sve u roku od 30 dana nakon primitka računa i u skladu s pravilima financijskog poslovanja korisnika Državnog proračuna.