Tehnička specifikacija

Nabava sustava za jednostavnu autentifikaciju (FI)

Sadržaj

[1. Uvod 2](#_Toc67658840)

[2. Sustav za upravljanje elektroničkim identitetima korisnika 2](#_Toc67658841)

[3. Sažeti opis 3](#_Toc67658842)

[4. Korisnici 3](#_Toc67658843)

[5. Upravljanje FIDO2 uređajima 3](#_Toc67658844)

[6. Komunikacija sa AAI@EduHr sustavom 3](#_Toc67658845)

[7. Bilježenje obavljenih akcija u sustavu (log) 4](#_Toc67658846)

[8. Isporuke 4](#_Toc67658847)

[9. Naknadne prilagodbe sustava (adaptivni sati) 5](#_Toc67658848)

[10. Ostalo 5](#_Toc67658849)

# 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 nabava sustava za jednostavnu autentifikaciju (FI).

# Sustav za upravljanje elektroničkim identitetima korisnika

Sustav imeničke infrastrukture je izdvojeni sustav koji sadrži identitete korisnika i ustanova.

Sustav 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 imeničke infrastrukture jedan je 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/ .

# Sažeti opis

Sustav za upravljanje FIDO2 uređajima i elektroničkim identitetima treba omogućiti upravljanje FIDO2 uređajima: evidenciju, njihovu dodjelu korisnicima te komunikaciju sa AAI@EduHr sustavom.

Ovaj sustav zamišljen je kao samostalan, a sa drugim sustavima komunicira na sljedeće načine

* za komunikaciju sa AAI@EduHr sustavom koristi mogućnosti programskog sučelja (REST API) koji se odnose na [višestupanjsku autentikaciju](https://www.aaiedu.hr/o-sustavu/sto-je-aaieduhr/visestupanjska-autentikacija).

# Korisnici

Korisnici ove aplikacije su:

* školski administratori
* CARNET administratori

# Upravljanje FIDO2 uređajima

Potrebno je osmisliti i omogućiti raspolaganje uređajima u sustavu, dohvatom iz postojećeg sustava za upravljanje resursima (ERP) i dodjelu željenog broja uređaja po školama. Također je potrebno osmisliti i omogućiti proces zaduživanja uređaja prema krajnjem korisniku (prema serijskom broju ili na neki drugi način), te na temelju toga prikazati stanje i statistiku zaduženja uređaja prema korisniku, odnosno određenoj školi.

Uz navedeno, potrebno je predvidjeti i osmisliti i mogućnost evidencije i raspolaganja FIDO2 uređajima koje je nabavio CARNET, škola ili pojedinac (korisnik), a koje prihvaća sustav AAI@EduHr.

Kroz sustav je potrebno predvidjeti mogućnost uvoza popisa uređaja i izvoza zaduženja kroz csv datoteke. Proces upravljanja FIDO2 uređajima će biti detaljnije razrađen kroz detaljnu funkcionalnu specifikaciju.

# Komunikacija sa AAI@EduHr sustavom

AAI@EduHr na raspolaganje stavlja sljedeće akcije:

1. Povezivanje elektroničkog identiteta sa FIDO2 uređajem
2. Poništavanje veze elektroničkog identiteta sa FIDO2 uređajem
3. Provjera FIDO2 statusa za određeni elektronički identitet
4. **Povezivanje elektroničkog identiteta sa FIDO2 uređajem**

Povezivanje elektroničkog identiteta (@skole.hr) za određenog korisnika može učiniti administrator ili korisnik samostalno.

Administrator sustava treba moći dodijeliti FIDO2 uređaj određenom korisniku u sustavu i povezivanje tog uređaja sa AAI@EduHr elektroničkim identitetom korisnika za kojeg je dodijeljen taj uređaj putem predviđene REST API akcije.

Nakon toga, uređaj treba biti predan direktno korisniku, uz uputu da pri prvoj FIDO2 autentikaciji treba provesti dvostupanjsku autentikaciju i tako potvrditi vezu svog uređaja i elektroničkog identiteta.

1. **Poništavanje veze elektroničkog identiteta sa FIDO2 uređajem**

Putem istog korisničkog sučelja i na sličan način kao i prilikom povezivanja, administrator sustava treba moći poništiti vezu AAI@EduHr elektroničkog identiteta sa FIDO2 uređajem, kao i po potrebi napraviti razduženje uređaja za odabranog korisnika.

Nakon poništavanja veze elektroničkog identiteta sa FIDO2 uređaja, za ponovnu aktivaciju FIDO2 uređaja ponovno je ponoviti postupak povezivanja, a nakon razduženja, uređaj (ako je ispravan) treba moći biti dodijeljen drugoj osobi.

1. **Provjera FIDO2 statusa za određeni elektronički identitet**

Prilikom pregleda korisnika u sustavu, korištenjem akcije za provjeru FIDO2 statusa, treba na adekvatan način (ikonom, tekstom, informacijom o datumu isteka valjanosti FIDO2 veze), prikazati status FIDO2 povezanosti za određenog korisnika.

Putem AAI@EduHr korisničkog portala (moj.aaiedu.hr), korisnik u svakom trenutku može vidjeti popis povezanih uređaja za svoj elektronički identitet, a prikaz statusa u administratorskom sučelju sustava za upravljanje FIDO2 uređajima treba odgovarati stanju iz sustava AAI@EduHr.

# Bilježenje obavljenih akcija u sustavu (log)

Sve navedene akcije koje se mogu izvršiti, trebaju biti zabilježene u zapisima (logovima) obavljenih akcija, zajedno sa opisom akcije, datumom, vremenom, korisničkim imenom te IP adresom korisnika (administratora) koji je učinio navedene promjene.

Akcije se trebaju moći pretraživati i sortirati prema svim navedenim atributima.

# Isporuke

Sve isporuke moraju biti usklađene i potvrđene od strane Naručitelja.

Planirane isporuke u sklopu nabave:

Detaljan projektni plan

Detaljna funkcionalna specifikacija

Detaljna tehnička specifikacija

Sustav za jednostavnu autentifikaciju (FI) s pripadajućom dokumentacijom

# Naknadne prilagodbe sustava (adaptivni sati)

Naknadne prilagodbe sustava isporučuje se sukladno pisanom nalogu Naručitelja temeljem Zahtjeva za promjenama i usuglašene procjene opsega posla. Odabrani ponuditelj daje procjenu broja čovjek/dana za predmetnu isporuku koju Naručitelj prihvaća ili odbija.

# Ostalo

Naručitelj ne snosi nikakav dodatan trošak licenci sustava za produkcijsku okolinu niti za repliku istog okruženja za potrebe testiranja i prihvaćanja korisničkih zahtjeva (UAT – User Acceptance Test).

Sve eventualne potrebne licence moraju biti isporučene, od strane odabranog ponuditelja, a bez vremenskih ograničenja i ograničenja broja korisnika.

Odabrani ponuditelj je dužan isporučiti jamstvo u trajanju od minimalno 5 (pet) godina na cjelokupno rješenje. Jamstvo uključuje ispravak svih uočenih nepravilnosti rada sustava te primjenu sigurnosnih zakrpi.

Također, prilikom razvoja IT rješenja, odabrani ponuditelj je dužan poštovati obaveze iz Dodatka „Obaveze odabranog ponuditelja u planiranju i razvoju IT rješenja“