

SVEUČILIŠTE U ZAGREBU
SVEUČILIŠNI RAČUNSKI CENTAR



**Provjera usklađenosti (certificiranje) matičnih
ustanova s normama Autentikacijske i autorizacijske
infrastrukture znanosti i visokog obrazovanja u
Republici Hrvatskoj - AAI@EduHr za 2022. godinu
(verzija 1.0)**



Zagreb, prosinac 2022.

U Zagrebu.

*KLASA: 650-03/22-005/003
URBROJ: 3801-5-005-01-22-6*

M.P.

*Predstojnik Sektora za posredničke sustave i
informacijsku sigurnost*

Mijo Đerek, dipl.ing

S A D R Ž A J

1. SUSTAV PROVJERE USKLAĐENOSTI (CERTIFICIRANJA)..... 4
2. POPIS NORMI ZA 2022. GODINU..... 5

1. SUSTAV PROVJERE USKLAĐENOSTI (CERTIFICIRANJA)

Sustav certificiranja definiran je dokumentom koji je javno dostupan na adresi https://www.aaiedu.hr/sites/default/files/content_files/docs/aaieduhr-idp-certificiranje-2009-v1.2.pdf.

Redovito godišnje certificiranje matičnih ustanova za 2022. godinu provodit će se u vremenu od 1. do 31. prosinca 2022. O eventualno potrebnom dopunskom roku Koordinator AAI@EduHr - Srce će obavijestiti matične ustanove nakon 2. siječnja 2023. Sukladno ranije spomenutom dokumentu provjeru provodi:

- Koordinator AAI@EduHr
 - automatizirano, uporabom odgovarajuće opreme i programskih alata,
 - pojedinačnim, neposrednim uvidom u aktivnosti subjekta,
 - uvidom u službenu dokumentaciju sustava AAI@EduHr;
- matična ustanova
 - popunjavanjem web obrasca na adresi <https://administracija.aaiedu.hr/subjekti/certificiranje/ustanova>,
 - instalacijom odgovarajućeg AOSI plug-ina za analizu sadržaja imenika, a prema uputama Koordinatora.

Koordinator ima pravo, neposrednim uvidom u stanje, provjeriti rezultate koje je subjekt ostvario samoprovjerom.

Sve matične ustanove dužne su sudjelovati u procesu provjere.

U sustavu AAI@EduHr utvrđene su 3 razine usklađenosti s normama AAI@EduHr:

- **razina 1: dovoljna usklađenost**
- **razina 2: dobra usklađenost**
- **razina 3: izvrsna usklađenost.**

Subjekt ima razinu usklađenosti 1 ukoliko pri provjeri zadovolji sve obavezne norme.

Subjekt ima razinu usklađenosti 2 ukoliko pri provjeri zadovolji sve obavezne i barem 50% preporučenih normi.

Subjekt ima razinu usklađenosti 3 ukoliko pri provjeri zadovolji sve obavezne i preporučene norme.

Temeljem provedene provjere Koordinator će utvrditi razinu usklađenosti te obavijest o tome pisanim putem dostaviti čelniku matične ustanove i objaviti putem web sjedišta na adresi <https://www.aaiedu.hr/za-maticne-ustanove/certificiranje-maticnih-ustanova-u-sustavu-aaieduhr/>. Zbirni izvještaj o provedenom certificiranju Koordinator će dostaviti Savjetu AAI@EduHr i MZO-u.

Koordinator će, o nedovoljnoj usklađenosti sa sustavom AAI@EduHr, pisanim putem izvijestiti čelnike matičnih ustanova koje ne dosegnu razinu 1 ili ne sudjeluju u procesu provjere te im odrediti dodatni rok od mjesec dana za postizanje razine 1. Ne postigne li matična ustanova razinu 1 i nakon dodatnog roka, Koordinator podnosi Savjetu AAI@EduHr prijedlog za privremeno isključenje matične ustanove iz sustava AAI@EduHr. Privremeno isključena matična ustanova može biti ponovno uključena u sustav AAI@EduHr tek kad dostigne razinu 1.

2. POPIS NORMI ZA 2022. GODINU

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
1. Formalno članstvo	Je li potpisan, ovjeren i odobren odgovarajući zahtjev za članstvo u AAI@EduHr sustavu?	obavezno	Koordinator
2. Imenovani predstavnici	Jesu li imenovane ovlaštene osobe i predstavnik u Vijeću AAI@EduHr te jesu li Koordinatoru dostavljeni ispravni kontakt podaci tih osoba?	obavezno	Koordinator
3. Obavijest o privatnosti dostupna korisnicima	Je li ustanova izradila i objavila obavijest o privatnosti usklađenu s odredbama uredbe GDPR	obavezno	Matična ustanova (samoprovjerom)
4. Procedura za informacijsko održavanje imenika utvrđena	Je li utvrđena procedura za informacijsko održavanje imenika?	obavezno	Matična ustanova (samoprovjerom)
5. Procedura za informacijsko održavanje imenika javno dostupna	Je li procedura za informacijsko održavanje imenika utvrđena i javno dostupna?	preporučeno	Matična ustanova (samoprovjerom)
6. Informiranje korisnika	Jesu li korisnici informirani o svojim pravima i obavezama prilikom preuzimanja e-identiteta?	obavezno	Matična ustanova (samoprovjerom)
7. Postojanje evidencije	Vodi li matična ustanova evidenciju o dodijeljenim e-identitetima?	obavezno	Matična ustanova (samoprovjerom)
8. Kontakt podaci za korisnike	Jesu li kontakt podaci za korisnike objavljeni na adresi http://www.aaiedu.hr/statistika-i-stanje-sustava/maticne-ustanove/popis točni ?	obavezno	Matična ustanova (samoprovjerom)
9. Obuhvaćenost e-identitetima	Posjeduju li svi zaposlenici (uključeni u nastavni ili znanstvenoistraživački proces) i studenti e-identitete?	preporučeno	Matična ustanova (samoprovjerom)
10. Provjera identiteta osobe pri dodjeli	Obavlja li se dodjela e-identiteta na temelju dokumenta sa slikom ili kroz proces zapošljavanja/upisa?	obavezno	Matična ustanova (samoprovjerom)
11. Postupak uručjenja e-identiteta	Uručuju li se podaci o e-identitetu osobno ili pisanim putem (ne telefonom ili e-mailom)? Odnosi se i na promjenu lozinke.	obavezno	Matična ustanova (samoprovjerom)
12. Brisanje e-identiteta	E-identiteti osoba koje su prestale biti povezane s ustanovom se pravodobno i redovito se brišu (sukladno utvrđenoj proceduri).	obavezno	Matična ustanova (samoprovjerom)

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
13. Informacijska kvaliteta imenika - istekli e-identiteti (obavezno)	Je li broj e-identiteta koji su označeni kao istekli prije više od 3 mjeseca (u to se broje i studentski e-identiteti bez podatka o isteku) manji od 1% ukupnog broja korisnika u LDAP imeniku?	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
14. Informacijska kvaliteta imenika - istekli e-identiteti (preporučeno)	U LDAP imeniku nema nijedan e-identitet označen kao istekao prije više od 3 mjeseca (u to se broje i studentski e-identiteti bez podatka o isteku).	preporučeno	Koordinator (putem programa za analizu sadržaja imenika)
15. Informacijska kvaliteta imenika - elektroničke adrese (obavezno)	U LDAP imeniku svi e-identiteti imaju ispravan podatak o e-mail adresi.	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
16. Informacijska kvaliteta imenika - OIB	Uz svaki je e-identitet zabilježen odgovarajući OIB. Iznimka mogu biti samo korisnici kojima je vrijednost atributa hrEduPersonPrimaryAffiliation „gost“.	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
17. Informacijska kvaliteta imenika - brožčani identifikator	Vrijednost atributa brožčani identifikator osobe je jedinstvena na nivou ustanove.	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
18. Informacijska kvaliteta imenika - podaci o ustanovi (hrOrg atributi)	Jesu li podaci o ustanovi zapisani u org zapisu LDAP imenika potpuni i ispravni?	obavezno	Koordinator (putem programa za analizu sadržaja imenika)
19. Nadzor AAI@EduHr komponente	Koordinatoru je omogućen nadzor rada LDAP, RADIUS i AOSI-WS poslužitelja.	obavezno	Koordinator
20. Programska podrška - LDAP (obavezno)	Je li na poslužitelju ustanove instalirana i ispravno konfigurirana inačica LDAP programskog paketa novija ili jednaka inačici 2.4.47 s implementiranom podrškom za obaveznu promjenu zaporke (AAI@EduHr LDAP paket 2.4.47+srce10u2)?	obavezno	Koordinator
21. Programska podrška - LDAP (preporučeno)	Je li na poslužitelju ustanove instalirana i ispravno konfigurirana najnovija inačica LDAP programskog paketa iz distribucije AAI@EduHr (2.4.47+srce10u2) ili drugog odgovarajućeg programa?	preporučeno	Koordinator

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
22. Programska podrška - RADIUS (obavezno)	Je li na poslužitelju ustanove instalirana i ispravno konfigurirana inačica RADIUS programskog paketa novija ili jednaka inačici 3.0.17 (AAI@EduHr RADIUS paket 3.0.17+srce10u1)?	obavezno	Koordinator
23. Programska podrška - RADIUS (preporučeno)	Je li na poslužitelju ustanove instalirana i ispravno konfigurirana najnovija inačica RADIUS programskog paketa iz distribucije AAI@EduHr s podrškom za F-Ticks (3.0.17+srce10u1) ili drugog odgovarajućeg programa?	preporučeno	Koordinator
24. Programska podrška – AOSI - WS (obavezno)	Je li na poslužitelju ustanove instalirana i ispravno konfigurirana inačica AOSI web servisa novija ili jednaka inačici 3.10.0 (AAI@EduHr AOSI WS paket 3.10.0+srce10u1)?	obavezno	Koordinator
25. Programska podrška – AOSI - WS (preporučeno)	Je li na poslužitelju ustanove instalirana i ispravno konfigurirana posljednja inačica odgovarajućeg programskog paketa iz distribucije AAI@EduHr (AOSI WS paket 3.10.0+srce10u1)?	preporučeno	Koordinator
26. Sekundarni servisi	U produkciji su sekundarni LDAP, RADIUS i AOSI-WS.	preporučeno	Koordinator
27. Postojanje uputa i web sučelja za vlasnike e-identiteta	Postoji li web sučelje za vlasnike e-identiteta putem kojeg oni mogu promijeniti zaporku i ostale podatke koje im je dozvoljeno mijenjati (AOSI-web sučelje, ISVU web sučelje ili vlastito rješenje)?	obavezno	Koordinator
28. Certifikat RADIUS poslužitelja – ispravan i dostupan korisnicima	Certifikat RADIUS poslužitelja ustanove je ispravan i dostupan korisnicima kroz uporabu eduroam installera (installer.eduroam.hr)	obavezno	Koordinator
29. Elektronički identiteti izdaju se isključivo fizičkim osobama	Elektronički identitet u sustavu AAI@EduHr odnosno slog u imeniku s identifikatorom (DN-om) oblika uid=oznaka, dc=domena, dc=hr izdaje se isključivo fizičkim osobama	obavezno	Matična ustanova (samoprovjerom)
30. AOSI-WS ima ispravan certifikat	AOSI-WS koristi poslužiteljski certifikat dobiven putem CARNetove usluge TCS (ili drugi certifikat kojeg web-preglednici automatski prepoznaju). Ovaj se uvjet odnosi i na sekundarni AOSI-WS ukoliko ga ustanova koristi u produkciji	obavezno	Koordinator

Norma	Opis uvjeta koji se provjerava	Status	Provjerava
31. TLS (Transport Layer Security) protokol inačice 1.2 ili veće	Inačica TLS protokola za komunikaciju između AOSI -WS i klijenta prilikom uspostave SSL tunela je novija ili jednaka inačici 1.2.	preporučeno	Koordinator
32. TLS (Transport Layer Security) protokol inačic 1.2 ili veće	Inačica TLS protokola za komunikaciju između RADIUS poslužitelja i klijenta prilikom uspostave SSL tunela je novija ili jednaka inačici 1.2.	preporučeno	Koordinator
33. RADIUS poslužitelj ispravno isporučuje atribut CUI	RADIUS poslužitelj ustanove ispravno isporučuje RADIUS atribut CUI (<i>Chargeable-User-Identity</i>).	obavezno	Koordinator



(certificiranje2022_AAIEduHr_IP_.docx)